



Advanced Copyright Issues on the Internet

By David L. Hayes, Esq.*

FENWICK & WEST LLP

(updated versions of this work are regularly made available online at no charge at <https://www.fenwick.com/insights/publications/advanced-copyright-issues-on-the-internet>)

*Partner and past Chairman of the Intellectual Property Practice Group, Fenwick & West LLP, Mountain View & San Francisco, California. B.S.E.E. (Summa Cum Laude), Rice University (1978); M.S.E.E., Stanford University (1980); J.D. (Cum Laude), Harvard Law School (1984). An early version of this work appeared in David L. Hayes, “Advanced Copyright Issues on the Internet,” 7 Tex. Intell. Prop. L.J. 1 (Fall 1998). The author expresses appreciation to Matthew Becker for significant contributions to Section III.E (“Streaming and Downloading”).

© 1997-2023 David L. Hayes. All Rights Reserved.

(Updated through March 2022)

I.	INTRODUCTION.....	1
II.	RIGHTS IMPLICATED BY TRANSMISSION AND USE OF WORKS ON THE INTERNET	2
A.	The Right of Reproduction	2
1.	The Ubiquitous Nature of “Copies” on the Internet	3
2.	Whether Images of Data Stored in RAM Qualify as “Copies”	3
3.	The WIPO Treaties & the European Copyright Directive Are Unclear With Respect to Interim “Copies”	11
(a)	Introduction to the WIPO Treaties & the European Copyright Directive.....	11
(b)	The WIPO Copyright Treaty	13
(c)	The WIPO Performances and Phonograms Treaty	16
4.	The Requirement of Volition for Direct Liability.....	18
(a)	The Netcom Case.....	19
(b)	The MAPHIA Case	21
(c)	The Sabella Case	22
(d)	The Frena Case	24
(e)	The Webworld Case	25
(f)	The Sanfilippo Case.....	26
(g)	The Free Republic Case	26
(h)	The MP3.com Cases	28
(i)	The CoStar Case	32
(j)	The Ellison Case	33
(k)	Perfect 10 v. Cybernet Ventures	33
(l)	Field v. Google	34
(m)	Parker v. Google	35
(n)	The Cablevision Case	35
(o)	Arista Records v. Usenet.com	39
(p)	Quantum Systems v. Sprint Nextel.....	39
(q)	Arista Records v. Myxer	40
(r)	Disney Enterprises v. Hotfile	41
(s)	Perfect 10 v. Megaupload	43
(t)	Wolk v. Kodak Imaging Network	44
(u)	Fox Broadcasting v. Dish Network.....	44
(v)	Perfect 10 v. Giganews.....	56
(w)	Capitol Records v. ReDigi.....	62
(x)	Hearst Stations v. Aereo	64
(y)	In Re Autohop Litigation (Dish Network v. American Broadcasting)	64
(z)	Oppenheimer v. Allvoices.....	66
(aa)	The Supreme Court’s Aereo Decision	66
(bb)	Gardner v. CafePress	66
(cc)	Rosen v. eBay.....	68
(dd)	BWP Media v. T&S Software	68
(ee)	Williams-Sonoma v. Amazon.com.....	70
(ff)	Summary of Case Law.....	71

5.	The Reproduction Right Under WIPO Implementing Legislation.....	72
(a)	United States Legislation	72
(1)	The Digital Millennium Copyright Act.....	72
(2)	Legislation Not Adopted	73
(b)	The European Copyright Directive	74
6.	Peer-to-Peer File Sharing	79
(a)	BMG Music v. Gonzalez	79
(b)	Columbia Pictures v. Bunnell.....	81
(c)	Sony BMG Music Entertainment v. Tenenbaum.....	81
(d)	Capitol Records v. Thomas-Rasset	85
7.	The Immunity of the Audio Home Recording Act (AHRA).....	89
(a)	The Diamond Multimedia Case	89
(b)	The Napster Cases	89
(c)	The Aimster Case	89
(d)	Atlantic Recording Corp. v. XM Satellite Radio	90
8.	Fair Use Cases.....	93
(a)	Fox News v. TVEyes	93
B.	The Right of Public Performance.....	99
1.	Isochronous Versus Asynchronous Transmissions	100
2.	The Meaning of “Publicly”	101
3.	Live Nation Motor Sports v. Davis.....	102
4.	United States v. ASCAP.....	103
5.	The Cablevision Case.....	104
6.	Ringtones – In re Application of Cellco Partnership	106
7.	Arista Records v. Myxer	107
8.	Warner Bros. v. WTV Systems.....	108
9.	Capitol Records v. MP3tunes	111
10.	American Broadcasting v. Aereo.....	111
11.	The BarryDriller Case.....	128
12.	Fox v. FilmOn	130
13.	Hearst Stations v. Aereo.....	134
14.	Community Television of Utah v. Aereo	135
15.	CBS v. FilmOn	137
16.	Capitol Records v. Escape Media	139
17.	Fox Broadcasting v. Dish Network	139
18.	Disney Enterprises v. VidAngel.....	141
19.	Spanski Enterprises v. Telewizja Polska	141
C.	The Right of Public Display	143
1.	The Frena, Marobie-FL, Hardenburgh and Webbworld Cases.....	144
2.	Kelly v. Arriba Soft	145
3.	Ticketmaster v. Tickets.com.....	149
4.	Perfect 10 v. Google (aka Perfect 10 v. Amazon)	149
5.	Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey	161

6.	ICG-Internet Commerce Group, Inc. v. Wolf	163
7.	Perfect 10 v. Yandex.....	163
8.	Leader’s Inst. v. Jackson	165
9.	Goldman v. Breitbart News Network.....	166
10.	Nicklen v. Sinclair Broad. Grp.....	169
11.	The “Server Test” Versus the “Incorporation Test”	170
(a)	Cases Accepting or Applying the Server Test.....	171
(1)	Perfect 10 v. Google.....	171
(2)	Perfect 10 v. Yandex.....	171
(3)	Louis Vuitton v. Akanoc Solutions.....	171
(4)	Hunley v. Instagram	172
(b)	Cases Rejecting the Server Test, Distinguishing It, or Refusing to Adjudicate It.....	172
(1)	Leader’s Institute v. Jackson	172
(2)	Goldman v. Breitbart News Network.....	173
(3)	Free Speech Sys. v. Menzel	173
(4)	Sinclair v. Ziff Davis.....	174
(5)	McGucken v. Newsweek	175
(6)	Nicklen v. Sinclair Broad. Grp.....	177
D.	The Right of Public Distribution.....	177
1.	The Requirement of a “Copy”	178
(a)	Cases Addressing Whether Mere “Making Available” Is a Distribution	178
(1)	Cases Holding That Mere “Making Available” Is a Distribution	179
(i)	Playboy Enterprises v. Frena	179
(ii)	Playboy Enterprises v. Chuckleberry Publishing	179
(iii)	Playboy Enterprises v. Webbworld.....	179
(iv)	Marobie-FL v. National Association of Fire Equipment Distributors	180
(v)	A&M Records v. Napster	180
(vi)	Interscope Records v. Duty.....	180
(vii)	Warner Bros. Records v. Payne	181
(viii)	Universal City Studios v. Bigwood	181
(ix)	Motown Record Co. v. DePietro.....	182
(x)	United States v. Carani	182
(xi)	ICG-Internet Commerce Group v. Wolf.....	182
(xii)	Maverick Recording Co. v. Harper	182
(xiii)	Columbia Pictures v. Fung	183
(xiv)	SA Music v. Apple.....	184
(2)	Cases Holding That Mere “Making Available” Is Not a Distribution	185
(i)	Religious Technology Center v. Netcom	185
(ii)	In re Napster Copyright Litigation	186
(iii)	Perfect 10 v. Google	187
(iv)	Latin American Music Co. v. Archdiocese of San Juan	188

(v)	London-Sire Records v. Doe	188
(vi)	Elektra Entertainment Group v. Barker	190
(vii)	Atlantic Recording Corp. v. Howell	191
(viii)	Capitol Records v. Thomas	193
(ix)	Fox Broadcasting v. Dish Network	194
(x)	BMG v. Cox Communications	195
(xi)	Alticor v. UMG Recordings	195
(xii)	APL Microscopic v. United States	196
(xiii)	SA Music v. Amazon.com	197
(xiv)	Brittney Gobble Photography v. Sinclair Broadcasting	197
(xv)	Grecco v. Age Fotostock Am.	198
(3)	Cases Refusing To Decide the Issue	199
(b)	Other Cases Adjudicating the Scope of the Distribution Right	200
(1)	Hearst Stations v. Aereo	200
(2)	Fox Broadcasting v. Dish Network	201
2.	The Requirement of a “Public” Distribution	201
3.	The Requirement of a Rental or Transfer of Ownership	202
4.	The Right of Distribution Under the WIPO Treaties	202
5.	The Right of Distribution Under WIPO Implementing Legislation	204
(a)	United States Legislation	204
(b)	The European Copyright Directive	204
E.	The Right of Importation	204
F.	The New Right of Transmission and Access Under the WIPO Treaties	205
1.	The Right of Communication to the Public in the WIPO Copyright Treaty	205
2.	The Right of Making Available to the Public in the WIPO Performances and Phonograms Treaty	208
3.	The Right of Transmission and Access Under WIPO Implementing Legislation	209
(a)	United States Legislation	209
(b)	The European Copyright Directive	210
G.	New Rights and Provisions Under The Digital Millennium Copyright Act, the European Copyright Directive & Legislation That Did Not Pass	213
1.	Circumvention of Technological Measures and Rights Management Information Under the DMCA	213
(a)	Circumvention of Technological Protection Measures	214
(1)	Prohibition on Conduct	214
(i)	Exemptions Adopted by the Librarian of Congress	215
a.	Scope of the Network Connection Exemption – The TracFone Cases	249
(ii)	Epic Games v. Altmeyer	252
(iii)	Facebook v. Power Ventures	253
(iv)	Bose v. Zavala	253
(v)	MGE UPS Systems v. GE	254
(vi)	Granger v. One Call Lender Services	254

(vii)	Dish Network v. World Cable.....	254
(viii)	Eyepartner v. Kor Media Group.....	257
(ix)	Granger v. Dethlefs	257
(x)	D&J Optical v. Wallace	258
(xi)	NNG v. AVA Enterprises	258
(xii)	Ford Motor Co. v. Autel Intelligent Technology	260
(xiii)	VBConversions v. Gulf Coast Ventures.....	262
(xiv)	General Motors v. Dorman Products	262
(xv)	Disney Enterprises v. VidAngel	264
(xvi)	Synopsys v. Ubiquiti Networks	273
(xvii)	Digital Drilling Data Sys. v. Petrolink Servs.	274
(xviii)	Eclipse Gaming v. Antonucci.....	276
(xix)	Synopsys v. AzurEngine	277
(xx)	In re Dealer Mgmt. Sys. Antitrust Litig. – Secondary Liability Under Section 1201(a).....	277
(2)	Prohibition on Devices	279
(i)	Sony Computer Entertainment America v. Gamemasters.....	280
(ii)	The DirecTV Cases.....	281
a.	DirecTV, Inc. v. Borow	281
b.	DirecTV, Inc. v. Carrillo	281
(iii)	Sony Computer Entertainment America v. Divineo	281
(iv)	Ticketmaster L.L.C. v. RMG Technologies, Inc.	282
(v)	The Tracfone Cases	283
(vi)	Movida Communications, Inc. v. Haifa	284
(vii)	MDY Industries v. Blizzard Entertainment.....	284
(viii)	Coupons, Inc. v. Stottlemire	289
(ix)	CoxCom, Inc. v. Chafee	290
(x)	The DISH Network Cases	291
a.	Dish Network v. Sonicview	291
b.	Dish Network v. SatFTA	291
c.	Dish Network v. Dimarco	292
d.	Dish Network v. Sonicview	293
e.	Dish Network v. Alejandri	294
f.	Dish Network v. World Cable	294
g.	Dish Network v. Barnaby	294
(xi)	Realnetworks v. DVD Copy Control Association.....	295
(xii)	Apple v. Psystar	297
(xiii)	Blizzard Entertainment v. Reeves.....	299
(xiv)	The Craigslist Cases.....	300
a.	Craigslist v. Naturemarket	300
b.	Craigslist v. Mesiab	300
c.	Craigslist v. Hubert	301
d.	Craigslist v. Branley	302
e.	Craigslist v. Kerbel	302

(xv)	Echostar v. Viewtech	302
(xvi)	Adobe Systems v. Feather	303
(xvii)	NNG v. AVA Enterprises	303
(xviii)	Beco Dairy Automation v. Global Tech Systems	303
(3)	What Constitutes an Effective Technological Measure	304
(i)	Auto Inspection Services v. Flint Auto Auction	304
(ii)	Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey	305
(iii)	Apple v. Psystar	307
(iv)	Ticketmaster v. Prestige Entertainment	307
(v)	Philips N. Am. v. Summit Imaging	308
(4)	Whether Unauthorized Use of a Valid Password or Key Constitutes Circumvention	309
(i)	Cases Holding That It Does Constitute Circumvention	309
a.	321 Studios v. Metro Goldwyn Mayer	309
b.	Microsoft v. EEE Business	310
c.	Actuate v. IBM	310
(ii)	Cases Holding That It Does Not Constitute Circumvention	311
a.	I.M.S. Inquiry Management Systems v. Berkshire Management Systems	311
b.	Egilman v. Keller & Heckman	311
c.	R.C. Olmstead v. CU Interface	312
d.	Navistar v. New Baltimore Garage	313
e.	Digital Drilling Data Sys. v. Petrolink	313
f.	R. Christopher Goodwin & Assocs. v. Search, Inc.	313
(iii)	Cases Refusing to Decide the Issue	314
a.	Avaya v. Telecom Labs	314
(5)	No Requirements With Respect to Design of a Product; Other Rights Not Affected	314
(6)	Exemption for Nonprofit Organizations and Law Enforcement	316
(7)	Reverse Engineering for Interoperability	316
(i)	Universal City Studios Inc. v. Reimerdes	321
(ii)	Storage Technology Corporation v. Custom Hardware Engineering & Consulting	322
(iii)	Chamberlain Group, Inc. v. Skylink Technologies, Inc.	322
(iv)	Lexmark International, Inc. v. Static Control Components, Inc.	323
(v)	Davidson Assocs. v. Internet Gateway	323
(vi)	Sony Computer Entertainment America v. Divineo	328
(vii)	Register of Copyrights' Report on Section 1201	328
(viii)	Authenticom v. CDK Global	329
(8)	Encryption Research	330
(9)	Protection of Minors	330
(10)	Protection of Personally Identifying Information	331

(11)	Security Testing	331
(12)	Copy Restrictions To Be Built Into VCRs and Camcorders.....	331
(13)	Other Cases Filed Under the Anti-Circumvention Provisions	332
(i)	Sony Computer Entertainment, Inc. v. Connectix, Inc.	332
(ii)	RealNetworks, Inc. v. Streambox Inc.	333
(iii)	Universal City Studios, Inc. v. Reimerdes	337
(iv)	A Related DVD Case Involving Trade Secret Claims – DVD Copy Control Association, Inc. v. McLaughlin (the Bunner case)	342
(v)	A Related DVD Case – Norwegian Prosecution of Jon Johansen	346
(vi)	Another Challenge to the DMCA – The Felten Case.	346
(vii)	Pearl Investments, LLC v. Standard I/O, Inc.	347
(viii)	321 Studios v. Metro Goldwyn Mayer Studios, Inc.	348
(ix)	Paramount Pictures Corp. v. 321 Studios.....	350
(x)	Macrovision Corp. v. 321 Studios.....	350
(xi)	Comcast of Illinois X v. Hightech Electronics, Inc.	350
(xii)	Davidson & Assocs. v. Internet Gateway.....	351
(xiii)	Agfa Monotype Corp. v. Adobe Sys.	351
(xiv)	Macrovision v. Sima Products Corp.....	354
(xv)	Nordstrom Consulting, Inc. v. M&S Technologies, Inc.	355
(xvi)	Dice Corp. v. Bold Technologies	355
(14)	Criminal Prosecutions Under the DMCA	356
(i)	The Sklyarov/Elcomsoft Case.....	356
(ii)	Other Criminal Prosecutions Under the DMCA.....	357
(iii)	The Requirement of Willfulness – Deliberate Ignorance.....	358
(15)	Other Uses of the Anti-Circumvention Provisions as a Sword	360
(i)	Lexmark International, Inc. v. Static Control Components, Inc.	360
(ii)	Chamberlain Group, Inc. v. Skylink Technologies, Inc.	367
(iii)	In re Certain Universal Transmitters for Garage Door Openers.....	373
(iv)	Storage Technology Corporation v. Custom Hardware Engineering & Consulting	374
(16)	Whether Fair Use Constitutes a Defense to Section 1201.....	378
(i)	Universal City Studios v. Corley	379
(ii)	321 Studios v. Metro Goldwyn Mayer Studios.....	379
(iii)	Macrovision v. Sima Products Corp.....	379
(iv)	The Sklyarov/Elcomsoft Case.....	379
(v)	Eyepartner v. Kor Media Group.....	379
(vi)	Disney Enterprises v. VidAngel	380
(vii)	Sony Computer Entertainment America v. Divineo	380
(viii)	Dish Network v. SatFTA.....	380
(ix)	Dish Network v. Sonicview.....	380

(x)	Realnetworks v. DVD Copy Control Association.....	380
(xi)	Apple v. Corellium.....	380
(17)	Register of Copyrights’ Report on Section 1201	383
(b)	Integrity of Copyright Management Information	383
(1)	Definition of CMI	383
(i)	Cases Requiring CMI to be Part of a Technological System or Process.....	384
a.	The IQ Group, Ltd. v. Wiesner Publishing, LLC.....	384
b.	Textile Secrets Int’l, Inc. v. Ya-Ya Brand Inc.	386
c.	Jacobsen v. Katzer	388
d.	Silver v. Lavadeira	389
(ii)	Cases Not Requiring CMI to be Part of a Technological System or Process	389
a.	McClatchey v. The Associated Press	389
b.	Associated Press v. All Headline News Corp.	390
c.	Fox v. Hildebrand	390
d.	Faulkner Press v. Class Notes.....	391
e.	Interplan Architect v. C.L. Thomas.....	392
f.	Agence France Presse v. Morel.....	392
g.	Murphy v. Millennium Radio.....	394
h.	William Wade Waller Co. v. Nexstar Broadcasting.....	396
i.	Leveyfilm v. Fox Sports.....	396
j.	Williams v. Roberto Cavalli S.p.A.....	397
k.	Bounce Exchange v. Zeus Enterprise	397
l.	Carter v. Pallante	399
m.	Preston Wood & Assocs v. RZ Enters. USA	399
n.	etrailer Corp. V. TexTrail, Inc.....	400
o.	Kobi Karp Architecture v. O’Donnell Dannwolf and Partners	400
p.	Sheung Wan Gallery Ltd. v. Kagan	401
(iii)	Cases Refusing to Decide the Issue	401
a.	Aaberg v. Francesca’s Collections	401
(iv)	Other Cases Construing the Definition of CMI.....	402
a.	Empire Med. Review Servs. V. CompuClaim, Inc.	402
b.	Maule v. Anheuser Busch	403
c.	SellPoolSuppliesOnline.com v. Ugly Pools Arizona	404
d.	Alan Ross Mach. v. Machinio	405
e.	Mango v. BuzzFeed	406
f.	Roth v. Walsh Co.	407
g.	etrailer Corp. v. Automatic Equip. Mfg.	408
h.	Energy Intelligence Grp. v. Kayne Anderson Capital Advisors	409
i.	Mills v. Netflix	409
j.	Hong v. Recreational Equipment	410

k.	Advanta-Star Auto. Research v. Reynolds Ford	411
l.	Yellow Pages Photos v. Dex Media.....	411
(2)	Prohibitions on False CMI and Removal/Alteration of CMI	412
(i)	Cases re Removal or Alteration of CMI	412
a.	Kelly v. Arriba Soft Corp.	412
b.	Thron v. Harper Collins Publishers	413
c.	Gordon v. Nextel Communications	414
d.	Monotype Imaging, Inc. v. Bitstream Inc.	415
e.	Keogh v. Big Lots Corp.	417
f.	Goldman v. Healthcare Management Systems	417
g.	Thomas M Gilbert Architects v. Accent Builders	418
h.	Banxcorp v. Costco	418
i.	Agence France Presse v. Morel	419
j.	Scholz Design v. Custom Homes	420
k.	Personal Keepsakes v. PersonalizationMall.com	420
l.	Frost-Tsuji Architects v. Highway Inn.....	422
m.	Tomelleri v. Zazzle, Inc.	423
n.	Iconics v. Massaro	427
o.	Stevens v. CoreLogic	428
p.	Friedman v. Live Nation Merchandise	431
q.	Robert L. Stark Enterprises v. Neptune Design Group.....	433
r.	Gattoni v. Tibi, LLC	434
s.	The Art of Design v. Pontoon Boat.....	434
t.	Fischer v. Forrest	435
u.	Philpot v. Alternet Media	437
v.	Design Basics v. Ashford Homes	438
w.	Design Basics v. WK Olson Architects	439
x.	FurnitureDealer.net v. Amazon.....	439
y.	GC2 v. Int’l Game Tech.	441
z.	Soos & Associates v. Five Guys Enterprises	442
aa.	Dominick R. Pilla v. Gilat	442
bb.	Philips N. Am. v. Summit Imaging	443
cc.	Bell v. Worthington City Sch. Dist.	444
dd.	RAZ Imports v. Regency Int’l Bus. Corp.....	444
ee.	Neo4j v. Graph Foundation	445
ff.	Munro v. Fairchild Tropical Botanic Garden	447
(ii)	Cases re False CMI	447
a.	Schiffer Publishing, Ltd. v. Chronicle Books, LLC	447
b.	Agence France Presse v. Morel	448
c.	Personal Keepsakes v. PersonalizationMall.com	449
d.	Drauglis v. Kappa Map Group	449
e.	Stevens v. CoreLogic	450
f.	GC2 v. Int’l Game Tech.....	450
g.	Pierson v. Infinity Music & Entm’t.....	452

h.	Zuma Press v. Getty Images	453
i.	Michael Grecco Prods v. Alamy.....	454
j.	Soos & Associates v. Five Guys Enterprises	455
k.	Michael Grecco Prods. v. Time USA.....	456
(3)	Exceptions and Limitations	457
(c)	Remedies for Violations of Sections 1201 and 1202	457
(1)	Statutory Damages and Disgorgement of Profits for Violations of Section 1201.....	458
(i)	Sony Computer Entertainment America v. Filippiak	458
(ii)	Sony Computer Entertainment v. Divineo	459
(iii)	Stockwire Research Group v. Lebed.....	460
(iv)	MDY Industries, LLC v. Blizzard Entertainment, Inc.	460
(v)	Nexon America v. Kumar	460
(vi)	Point 4 Data Corp. v. Tri-State Surgical Supply.....	461
(2)	Statutory Damages and Disgorgement of Profits for Violations of Section 1202.....	464
(i)	McClatchey v. The Associated Press.....	464
(ii)	Goldman v. Healthcare Management Systems.....	465
(iii)	Stockwire Research Group v. Lebed.....	466
(iv)	Stockart.com v. Engle	466
(v)	Granger v. One Call Lender Services	467
(vi)	Pacific Stock v. MacArthur & Co.	467
(vii)	Agence France Presse v. Morel	468
(viii)	Reilly v. Plot Commerce	469
(3)	Whether There is a Right to Jury Trial on Statutory Damages Under Section 1202	471
(i)	Oppenheimer v. Johnson.....	471
(ii)	Huffman v. Activision Publ'g.....	471
(4)	Whether Copyright Registration is a Prerequisite to a DMCA Claim or Remedies	472
(i)	Design Ideas v. Meijer.....	472
(ii)	Diamondback Indus. v. Repeat Precision	472
(5)	Whether Mitigation is a Defense to Statutory Damages Under the DMCA	473
(i)	Energy Intelligence Grp. v. Kayne Anderson Capital Advisors.....	473
(6)	Statute of Limitations.....	475
(7)	Jurisdictional Issues – Blueport Co. v. United States.....	475
(8)	Arbitrability of Claims Under the DMCA.....	475
(d)	Alternative Approaches to the DMCA That Did Not Pass	476
(e)	The Battle Between Content Owners and Technology Companies Over Built-In Technological Measures	477
2.	Anticircumvention Provisions Under the European Copyright Directive.....	478
3.	Anti-Circumvention Provisions in Other Foreign Countries	481

4.	Fair Use	482
(a)	United States Legislation That Did Not Pass	482
(b)	The European Copyright Directive	482
5.	Expansion of Library/Archives Exemptions.....	483
6.	Distance Education.....	484
7.	Copying in the Course of Computer Maintenance or Repair	484
8.	Other Provisions of the DMCA.....	485
(a)	Evaluation of Impact of Copyright Law on Electronic Commerce	485
(b)	Clarification of the Authority of the Copyright Office.....	486
(c)	Ephemeral Recordings.....	487
(d)	Statutory Licenses With Respect to Performances of Sound Recordings	487
(e)	Assumption of Contractual Obligations Related to Transfers of Rights in Motion Pictures	487
(f)	Protection of Certain Industrial Designs	488
(1)	Protection of Designs Embodied in Useful Articles.....	488
(2)	Originality	489
(3)	Exclusions from Protection	489
(4)	Adaptations of Unprotectable Elements	490
(5)	Duration of Protection and Design Notice	490
(6)	Rights of a Design Owner and Limitations.....	490
(7)	Standard of Infringement	491
(8)	Benefit of Foreign Filing Date	491
(9)	Vesting and Transfer of Ownership	492
(10)	Remedies of Injunctive Relief, Damages, Attorneys' Fees and Destruction.....	492
(11)	Private Rights of Action Against Pirated Designs	492
(12)	Relation to Design Patents and Retroactive Effect	492
(g)	Limitation of Liability of Online Service Providers	493
(h)	Subpoenas to Service Providers	493
(1)	Jurisdictional Issues.....	493
(2)	RIAA v. Verizon Internet Services	494
(3)	The Charter Communications Litigation.....	497
(4)	Fatwallet v. Best Buy	498
(5)	In re Subpoena to University of North Carolina at Chapel Hill.....	498
(6)	Subpoenas in John Doe Actions.....	499
(7)	Interscope Records v. Does 1-7	501
(8)	In re Maximized Living	501
(9)	In re Subpoena Issued to Birch Communications	501
(10)	In re DMCA Subpoena Issued to eBay, Inc.	502
(11)	In re DMCA Subpoena to Reddit, Inc.	502
(12)	In re DMCA Section 512(h) Subpoena to YouTube (Google, Inc.).....	503
9.	Proposed Limitation of Scope of Shrinkwrap and Clickwrap Licenses That Did Not Pass.....	503
III.	APPLICATION OF COPYRIGHT RIGHTS TO SPECIFIC ACTS ON THE INTERNET	505

A. Browsing	505
B. Caching	507
1. Types of Caching	507
2. The Detriments of Caching	508
3. The Netcom Case and Application of the Fair Use Doctrine	510
(a) Purpose and Character of the Use	510
(b) Nature of the Copyrighted Work	511
(c) Amount and Substantiality of the Portion Used	511
(d) Effect of Use on the Potential Market	512
4. Cases Adjudicating Caching Under the Fair Use and Implied License Doctrines	514
(a) Field v. Google	514
(b) Perfect 10 v. Google (aka Perfect 10 v. Amazon).....	518
(c) Ticketmaster L.L.C. v. RMG Technologies, Inc.....	519
(d) Parker v. Yahoo!, Inc.....	520
5. Other Caching Cases	521
(a) Facebook v. Power Ventures.....	521
C. Liability of Online Service Providers	521
1. Direct Liability.....	521
(a) Louis Vuitton v. Akanoc Solutions	522
(b) Flava Works v. Gunter	523
(c) Capitol Records v. Escape Media	524
(d) UMG Recording v. Escape Media	528
(e) Milo & Gabby v. Amazon.com	530
(f) Smith v. Barnesandnoble.com.....	530
(g) BWP Media v. Polyvore	532
(h) Live Face on Web v. Biblio Holdings.....	536
(i) VHT v. Zillow Group	538
(j) Atari v. Redbubble	550
2. Contributory Liability.....	553
(a) The Netcom Case.....	553
(b) The MAPHIA Case	554
(c) The Peer-to-Peer Filing Sharing Cases	555
(1) The Napster Cases.....	555
(2) The Scour.com Lawsuit	591
(3) The Aimster/Madster Lawsuits.....	592
(4) The StreamCast/Kazaa/Grokster Lawsuits	598
(5) The Supreme Court's Grokster Decision	606
(6) The Grokster Decision on Remand	621
(i) The Ruling on Liability	621
(ii) The Permanent Injunction	625
(7) The Audiogalaxy Case	629
(8) The Hummer Winblad/Bertelsmann Litigation	629

(9) Arista Records v. Lime Group.....	633
(d) The CoStar Case	633
(e) Ellison v. Robertson	633
(f) Perfect 10 v. Cybernet Ventures	634
(g) Perfect 10 v. Visa International	636
(h) Parker v. Google	637
(i) MDY Industries v. Blizzard Entertainment	638
(j) Louis Vuitton v. Akanoc Solutions, Inc.	640
(k) Arista Records v. Usenet.com	643
(l) Hermeris v. Brandenburg	644
(m) Flava Works v. Gunter	645
(n) Perfect 10 v. Giganews	648
(o) Masck v. Sports Illustrated	657
(p) Rosen v. Global Net Access	658
(q) Capitol Records v. Escape Media	659
(r) UMG Recording v. Escape Media	659
(s) Fox Broadcasting v. Dish Network.....	659
(t) Smith v. Barnesandnoble.com.....	659
(u) Hart v. Amazon.com, Inc.	660
(v) Tomelleri v. Zazzle, Inc.....	660
(w) BMG v. Cox Communications	660
(x) Live Face on Web v. The Control Media Group	678
(y) BWP Media v. Polyvore	679
(z) VHT v. Zillow Group	679
(aa) UMG Recordings v. Grande Communications Networks	679
(bb) Cobbler Nevada v. Gonzales.....	682
(cc) Erickson Prods. v. Kast	685
(dd) Oppenheimer v. Morgan	687
(ee) King v. Amazon	688
(ff) Sony Music v. Cox Communications.....	689
(gg) ALS Scan v. Steadfast Networks	691
(hh) Atari v. Redbubble	692
(ii) Mon Cheri Bridals v. Cloudflare.....	693
(jj) Some Observations.....	693
3. Vicarious Liability.....	696
(a) The Netcom Case and its Progeny	696
(b) The Napster Cases	697
(c) Ellison v. Robertson	697
(d) Perfect 10 v. Cybernet Ventures	697
(e) The Aimster/Madster Lawsuits	698
(f) The StreamCast/Kazaa/Grokster Lawsuits	699
(g) Perfect 10 v. Visa International	701
(h) Parker v. Google	703
(i) Louis Vuitton v. Akanoc Solutions	704

(j)	Live Face on Web v. Howard Stern Productions.....	704
(k)	Arista Records v. Usenet.com	705
(l)	Corbis v. Starr.....	706
(m)	Arista Records v. Lime Group	706
(n)	Hermeris v. Brandenburg	706
(o)	Luvdarts v. AT&T Mobility	706
(p)	Flava Works v. Gunter	708
(q)	Perfect 10 v. Giganews.....	708
(r)	Masck v. Sports Illustrated	708
(s)	Disney Enterprises v. Hotfile	708
(t)	Capitol Records v. Escape Media	709
(u)	UMG Recording v. Escape Media	709
(v)	Gardner v. CafePress	709
(w)	BMG v. Cox Communications.....	709
(x)	GC2 v. Int’l Game Tech.	709
(y)	VHT v. Zillow Group	710
(z)	UMG Recordings v. Grande Communications Networks.....	710
(aa)	Erickson Prods v. Kast.....	710
(bb)	UMG Recordings v. Bright House Networks	710
(cc)	Atari v. Redbubble	711
4.	Inducement Liability.....	711
(a)	The Supreme Court’s Grokster Decision	711
(b)	Arista Records v. Usenet.com	712
(c)	Columbia Pictures v. Fung	713
(d)	Arista Records v. Lime Group	718
(e)	Flava Works v. Gunter	724
(f)	Disney Enterprises v. Hotfile	724
(g)	UMG Recording v. Escape Media	726
5.	Adequacy of Pleadings of Secondary Liability Against Service Providers	726
(a)	Miller v. Facebook	726
(b)	Williams v. Scribd.....	727
(c)	ALS Scan v. Cloudflare	728
(d)	Warner Records v. Charter Communications	729
6.	Limitations of Liability of Online Service Providers in the DMCA.....	730
(a)	History of the Various Legislative Efforts	731
(b)	The OSP Liability Provisions of the DMCA.....	732
(1)	Safe Harbors – Definition of a “Service Provider”	733
(i)	Acting as a Mere Conduit for Infringing Information – Section 512(a)	733
a.	The Napster Case	734
b.	Ellison v. Robertson	737
c.	The Aimster/Madster Lawsuits	742
d.	Perfect 10 v. CCBill	743
e.	Columbia Pictures v. Fung	751

f.	American Broadcasting v. Aereo	752
g.	Rosen v. Global Net Access	752
h.	BMG v. Cox Communications.....	752
(ii)	Caching – Section 512(b)	766
a.	Field v. Google	768
b.	Parker v. Google	769
c.	Perfect 10 v. Google	770
(iii)	Innocent Storage of Infringing Information – Section 512(c)	774
a.	The ALS Scan Case – What Constitutes a “Substantially” Compliant Notice	777
b.	Hendrickson v. eBay	780
c.	CoStar v. LoopNet	784
d.	Perfect 10 v. Cybernet Ventures.....	793
e.	The Aimster/Madster Lawsuits	796
f.	Hendrickson v. Amazon.com.....	796
g.	Rossi v. MPAA	798
h.	Perfect 10 v. CCBill	800
i.	Corbis Corp. v. Amazon.com, Inc.	801
j.	Tur v. YouTube, Inc.	807
k.	Io Group v. Veoh Networks.....	808
l.	UMG Recordings v. Veoh Networks (aff’d sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC)	812
m.	Perfect 10 v. Amazon	827
n.	Louis Vuitton v. Akanoc Solutions	829
o.	Viacom v. YouTube	829
p.	Perfect 10 v. Google	841
q.	Wolk v. Kodak Imaging Network	841
r.	Arista Records v. Myxer	845
s.	Flava Works v. Gunter	849
t.	Capitol Records v. MP3tunes	849
u.	Obodai v. Demand Media	864
v.	Agence France Presse v. Morel	865
w.	Columbia Pictures v. Fung	872
x.	Ventura Content v. Motherless.....	875
y.	Disney Enterprises v. Hotfile	886
z.	Capitol Records v. Vimeo	888
aa.	Perfect 10 v. Giganews	900
bb.	Rosen v. Global Net Access	902
cc.	Mavrix Photographs v. LiveJournal	903
dd.	Rosen v. eBay	908
ee.	Capitol Records v. Escape Media	910
ff.	BWP Media v. Clarity Digital.....	913
gg.	Milo & Gabby v. Amazon.com.....	917

hh. Hempton v. Pond5	918
ii. Greg Young Publishing v. Zazzle	920
jj. Long v. Dorset	922
kk. Downs v. Oath	924
ll. Feingold v. RageOn	925
mm. Williams-Sonoma v. Amazon.com	925
nn. Atari v. Redbubble	925
(iv) Referral or Linking to Infringing Material (Information Location Tools) – Section 512(d)	926
a. The Napster Case	927
b. Perfect 10 v. Cybernet Ventures	928
c. The MP3Board Case	928
d. The Aimster/Madster Lawsuits	928
e. The Diebold Lawsuit	929
f. Perfect 10 v. CCBill	932
g. Columbia Pictures v. Fung	933
h. Perfect 10 v. Google	934
i. Perfect 10 v. Yandex	934
(2) General Requirements for Limitations of Liability	935
(i) What Constitutes a “Standard Technical Measure”	936
a. Perfect 10 v. CCBill	936
b. Wolk v. Kodak Imaging Networks	936
c. Obodai v. Demand Media	937
d. Capitol Records v. Vimeo	937
e. BWP Media v. Polyvore	937
(3) Special Provisions for Nonprofit Educational Institutions	938
(4) Filing of False DMCA Notices – Section 512(f)	938
(i) Rossi v. MPAA	939
(ii) Online Policy Group v. Diebold, Inc.	939
(iii) Dudnikov v. MGA Entertainment	939
(iv) Novotny v. Chapman	939
(v) BioSafe-One, Inc. v. Hawks	940
(vi) Lenz v. Universal Music Corp.	941
(vii) UMG Recordings v. Augusto	950
(viii) Capitol Records v. MP3tunes	951
(ix) Brave New Films v. Weiner	952
(x) Cabell v. Zimmerman	952
(xi) Design Furnishings v. Zen Path	953
(xii) Amaretto Ranch Breedables v. Ozimals	954
(xiii) Shropshire v. Canning	954
(xiv) Rock River Communications v. Universal Music Group	955
(xv) Smith v. Summit Entertainment	956
(xvi) Ouellette v. Viacom	956

(xvii)	Tuteur v. Crosley-Corcoran.....	958
(xviii)	Flava Works v. Gunter.....	959
(xix)	Disney Enterprises v. Hotfile.....	960
(xx)	Flynn v. Siren-Bookstrand.....	961
(xxi)	Crossfit v. Alvies (based on a trademark claim under the DMCA).....	962
(xxii)	Automattic v. Steiner.....	963
(xxiii)	Distribuidora v. Guerra.....	964
(xxiv)	Handshoe v. Perret.....	966
(xxv)	ISE Entertainment v. Longarzo.....	966
(xxvi)	Stevens v. Vodka & Milk.....	966
(xxvii)	Johnson v. New Destiny Christian Center Church.....	967
(xxviii)	Ningbo Mizhihe v. Does.....	968
(xxix)	Enttech Media Grp. V. Okularity.....	969
(xxx)	Warner Records v. Charter Communications.....	970
(xxxi)	The Sunny Factory v. Chen.....	971
(xxxii)	Business Casual Holdings v. TV-Novosti.....	972
(5)	Filing of False DMCA Counternotices – Section 512(g)(3)(C).....	972
(i)	Hosseinzadeh v. Klein.....	972
(6)	Other Provisions.....	973
(7)	Injunctions Against Service Providers.....	974
(8)	Designation of Agent to Receive Notification of Claimed Infringement.....	974
(i)	CoStar v. Loopnet.....	976
(ii)	Wolk v. Kodak Imaging Network.....	976
(iii)	Perfect 10 v. Yandex.....	977
(iv)	Oppenheimer v. Allvoices.....	977
(v)	BWP Media v. Hollywood Fan Sites.....	977
(vi)	Van Stry v. McCrea.....	978
(9)	Whether the Safe Harbors Apply to Pre-1972 Sound Recordings.....	979
(i)	Cases Concluding the Safe Harbors Apply to Pre-1972 Sound Recordings.....	979
(ii)	Cases Concluding the Safe Harbors Do Not Apply to Pre- 1972 Sound Recordings.....	982
(10)	Applicability of the Communications Decency Act to Pre-1972 Sound Recordings.....	983
7.	Limitations of Liability of Online Service Providers under the Communications Decency Act.....	983
(a)	Stoner v. eBay.....	984
(b)	Perfect 10 v. CCBill.....	985
8.	Secondary Liability of Investors.....	986
(a)	The Hummer Winblad/Bertelsmann Litigation.....	986
(b)	UMG Recordings v. Veoh Networks.....	986
9.	Class Actions.....	988

D. Linking and Framing	988
1. The Shetland Times Case	991
2. The Total News Case	992
3. The Seattle Sidewalk Case.....	994
4. The Futuredontics Case.....	995
5. The Bernstein Case.....	996
6. The Intellectual Reserve Case	997
7. Ticketmaster v. Tickets.com.....	998
8. The MP3Board Case	1001
9. Kelly v. Arriba Soft	1004
10. Batesville Services, Inc. v. Funeral Depot, Inc.....	1004
11. Live Nation Sports v. Davis	1006
12. Perfect 10 v. Google (aka Perfect 10 v. Amazon)	1007
13. Pearson Education v. Ishayev.....	1007
E. Streaming and Downloading	1008
1. The Digital Performance Right – The Section 114(d)(1) Exemption and Streaming by FCC-Licensed Broadcasters.....	1008
2. The Digital Performance Right – Statutory Licenses Under Section 114 for Certain Nonsubscription and Subscription Services.....	1012
(a) Preexisting Subscription Services	1015
(b) Eligible Nonsubscription Services (Webcasters).....	1021
(c) New Subscription Services	1032
3. The Digital Performance Right – What Constitutes an “Interactive” Service	1036
(a) Arista Records v. Launch Media	1038
4. The Reproduction Right – Mechanical Licenses and Streaming/Downloading ..	1040
(a) Applicability of the Section 115 Compulsory License to Streaming	1042
(1) Rodgers & Hammerstein Org’n v. UMG Recordings	1042
(2) ABKCO Music v. Sagan	1043
(b) The Copyright Office’s Position – The 2001 DMCA Report and Comment Proceedings	1045
(c) The NMPA/HFA/RIAA Agreement of 2001.....	1047
(d) The Interactive Streaming and Limited Download Agreement of 2008.....	1049
(e) 2008 Interim Regulation re Compulsory DPD License	1050
(f) Applicability of the Section 115 Compulsory License to Ringtones.....	1052
(g) Subsequent Determinations of Compulsory License Rates by the CRB	1052
5. The Section 111 Compulsory License for Cable Systems	1053
(a) WPIX v. ivi	1053
(b) CBS v. FilmOn	1053
(c) American Broadcasting v. Aereo	1054
(d) Fox Television v. AereoKiller.....	1054
(e) Fox Television v. FilmOn X	1058
(f) FilmOn X v. Window to the World Communications	1059
6. International Licensing Efforts	1060

F. First Sales in Electronic Commerce	1060
1. Capitol Records v. ReDigi	1063
G. Pop-Up Advertising.....	1067
1. The Gator Litigations.....	1067
2. The WhenU Litigations.....	1069
(a) U-Haul v. WhenU.com	1069
(b) Wells Fargo v. WhenU.com	1071
(c) 1-800 Contacts v. WhenU.com	1073
3. The MetroGuide Litigation.....	1076
4. The D Squared Litigation.....	1076
5. International Decisions	1077
H. Harvesting of Web Data	1077
1. The FatWallet Dispute.....	1077
2. Nautical Solutions Marketing v. Boats.com	1077
3. Craigslist v. 3Taps	1078
IV. CONCLUSION	1079

ADVANCED COPYRIGHT ISSUES ON THE INTERNET

I. INTRODUCTION

Over the years, the Internet has become the basic foundational infrastructure for the global movement of data of all kinds. With continued growth at a phenomenal rate, the Internet has moved from a quiet means of communication among academic and scientific research circles into ubiquity in both the commercial arena and private homes. The Internet is now a major global data pipeline through which large amounts of intellectual property are moved. As this pipeline is now regularly used in the mainstream of commerce to sell and deliver creative content and information across transnational borders, issues of intellectual property protection for the material available on and through the Internet have taken on great importance.

Copyright law provides one of the most important forms of intellectual property protection on the Internet for at least two reasons. First, much of the material that moves in commerce on the Internet is works of authorship, such as musical works, multimedia works, audiovisual works, movies, software, database information and the like, which are within the usual subject matter of copyright. Second, because the very nature of an electronic online medium requires that data be “copied” as it is transmitted through the various nodes of the network, copyright rights are obviously at issue.

Traditional copyright law was designed to deal primarily with the creation, distribution and sale of protected works in tangible copies.¹ In a world of tangible distribution, it is generally easy to know when a “copy” has been made. The nature of the Internet, however, is such that it is often difficult to know precisely whether a “copy” of a work has been made and, if so, where it resides at any given time within the network. As described further below, information is sent through the Internet using a technology known as “packet switching,” in which data is broken up into smaller units, or “packets,” and the packets are sent as discrete units. As these packets pass through the random access memory (RAM) of each interim computer node on the network, are “copies” of the work being made?

The case of MAI Systems Corp. v. Peak Computer² held that loading a computer program into the RAM of a computer constituted the making of a “copy” within the purview of copyright law. This case has been followed by a number of other courts. Under the rationale of this case, a “copy” may be created under United States law at each stage of transmission of a work through the Internet. The language of two treaties discussed extensively in this paper – the

¹ For example, under United States law, copyright protection subsists only in “works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.” 17 U.S.C. § 102(a).

² 991 F.2d 511 (9th Cir. 1993), cert. dismissed, 114 S. Ct. 672 (1994).

WIPO Copyright Treaty³ and the WIPO Performances and Phonograms Treaty⁴ – leave unclear the crucial question whether the MAI approach will be internationalized. In any event, these two treaties would strengthen copyright holders’ rights of “distribution” and would create new rights of “making available to the public” a copyrighted work, both of which are implicated by transmissions through the Internet nearly as broadly as the right of reproduction.

The ubiquitous nature of “copying” in the course of physical transmission gives the copyright owner potentially very strong rights with respect to the movement of copyrighted material through the Internet, and has moved copyright to the center of attention as a form of intellectual property on the Internet. If the law categorizes all interim and received transmissions as “copies” for copyright law purposes, or treats all such transmissions as falling within the right of distribution of the copyright owner, then activities that have been permissible with respect to traditional tangible copies of works, such as browsing and transfer, may now fall within the control of the copyright holder.

This work discusses the multitude of areas in which copyright issues arise in an online context. Although the issues will, for simplicity of reference, be discussed in the context of the Internet, the analysis applies to any form of online usage of copyrighted works. Part II of this work discusses the various copyright rights that may be implicated by transmissions and use of works on the Internet, including new rights and remedies, as well as certain limitations on liability for online service providers afforded under federal statutes. Part III then analyzes the application of those rights to various activities on the Internet, such as browsing, caching, operation of an online service or bulletin board, linking to other sites, creation of derivative works, and resale or subsequent transfer of works downloaded from the Internet. Part III also analyzes the application of the fair use doctrine and the implied license doctrine to various Internet activities. Because the law is constantly developing with respect to many of these issues, considerable uncertainty is likely to exist as the issues continue to be worked out over time through the courts and the various relevant legislative bodies and industry organizations.

II. RIGHTS IMPLICATED BY TRANSMISSION AND USE OF WORKS ON THE INTERNET

This Part discusses the various rights of the copyright holder – the right of reproduction, the right of public performance, the right of public display, the right of public distribution, the right of importation, and the new rights of transmission and access – that are implicated by the transmission and use of works on the Internet.

A. The Right of Reproduction

The single most important copyright right implicated by the transmission and use of works on the Internet is the right of reproduction. As elaborated below, if the law categorizes all

³ World Intellectual Property Organization Copyright Treaty, Apr. 12, 1997, S. Treaty Doc. No. 105-17 (1997).

⁴ World Intellectual Property Organization Performances and Phonograms Treaty, Apr. 12, 1997, S. Treaty Doc. No. 105-17 (1997).

interim and received transmissions as “copies” for copyright law purposes, then a broad range of ordinary activities on the Internet, such as browsing, caching, and access of information, may fall within the copyright holder’s monopoly rights.

1. The Ubiquitous Nature of “Copies” on the Internet

Under current technology, information is transmitted through the Internet using a technique known broadly as “packet switching.” Specifically, data to be transmitted through the network is broken up into smaller units or “packets” of information, which are in effect labeled as to their proper order. The packets are then sent through the network as discrete units, often through multiple different paths and often at different times. As the packets are released and forwarded through the network, each “router” computer makes a temporary (ephemeral) copy of each packet and transmits it to the next router according to the best path available at that instant, until it arrives at its destination. The packets, which frequently do not arrive in sequential order, are then “reassembled” at the receiving end into proper order to reconstruct the data that was sent.⁵ Thus, only certain subsets (packets) of the data being transmitted are passing through the RAM of a node computer at any given time, although a complete copy of the transmitted data may be created and/or stored at the ultimate destination computer, either in the destination computer’s RAM, on its hard disk, or in portions of both.

To illustrate the number of interim “copies,” in whole or in part, that may be made when transmitting a work through the Internet, consider the example of downloading a picture from a website. During the course of such transmission, no less than seven interim copies of the picture may be made: the modem at the receiving and transmitting computers will buffer each byte of data, as will the router, the receiving computer itself (in RAM), the Web browser, the video decompression chip, and the video display board.⁶ These copies are in addition to the one that may be stored on the recipient computer’s hard disk.⁷

2. Whether Images of Data Stored in RAM Qualify as “Copies”

Do these interim and final copies of a work (many of which are only partial) being transmitted through the Internet qualify as “copies” within the meaning of United States copyright law? The copyright statute defines “copies” as:

material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or

⁵ If any packet is lost along the way, the originating computer automatically resends it, likely along a different path than the lost packet was originally sent.

⁶ Mark A. Lemley, “Dealing with Overlapping Copyrights on the Internet,” 22 U. Dayton L. Rev. 547, 555 (1997).

⁷ Even if a complete copy of the picture is not intentionally stored on the recipient computer’s hard disk, most computers enhance performance of their memory by swapping certain data loaded in RAM onto the hard disk to free up RAM for other data, and retrieving the swapped data from the hard disk when it is needed again. Some of this swapped data may be left on the hard disk when the computer is turned off, even though the copy in RAM has been destroyed.

otherwise communicated, either directly or with the aid of a machine or device. The term “copies” includes the material object, other than a phonorecord, in which the work is first fixed.⁸

The language of the definition raises two issues concerning whether images⁹ of transmitted data in RAM qualify as “copies.” First, depending upon where the data is in transit through the Internet, only a few packets – or indeed perhaps only a single byte – of the data may reside in a given RAM at a given time. For example, the modem at the receiving and transmitting computers may buffer only one or a few bytes of data at a time. A node computer may receive only a few packets of the total data, the other packets being passed through a different route and therefore a different node computer’s RAM. Should the law consider these partial images a “copy” of the work? Should the outcome turn on whether all or most of the packets of data comprising the work pass through a given RAM, or only a portion? How can interim partial images of data stored in RAM be deemed a “copy” of a work, in the case where there is no point in time at which the entire work is available in a single RAM?

The White Paper published by the Working Group on Intellectual Property Rights of President Clinton’s Information Infrastructure Task Force (referred to herein as the “NII White Paper”) implicitly suggests that at least interim, partial copies of a work created in RAM in interim node computers during transmission may not themselves constitute a “fixed” copy:

A transmission, in and of itself, is not a fixation. While a transmission may result in a fixation, a work is not fixed by virtue of the transmission alone. Therefore, “live” transmissions via the NII [National Information Infrastructure] will not meet the fixation requirement, and will be unprotected by the Copyright Act, unless the work is being fixed at the same time as it is being transmitted.¹⁰

The second general issue raised by the definition of “copies” is whether images of data stored in RAM are sufficiently “permanent” to be deemed “copies” for copyright purposes. The definition of “copies” speaks of “material objects,” suggesting an enduring, tangible embodying medium for a work. With respect to an image of data stored in RAM, is the RAM itself to be considered the “material object”? The image of the data in RAM disappears when the computer is turned off. In addition, most RAM is “dynamic” (DRAM), meaning that even while the computer is on, the data must be continually refreshed in order to remain readable. So the data is in every sense “fleeting.” Is its embodiment in RAM sufficiently permanent to be deemed a “copy”?

⁸ 17 U.S.C. § 101.

⁹ The word “image” is being used here to refer to an image of data stored in RAM to avoid use of the word “copy,” which is a legal term of art. Whether an image of data in RAM should be deemed a “copy” for copyright law purposes is the question at issue.

¹⁰ Information Infrastructure Task Force, “Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights” at 27 (1995).

The legislative history of the Copyright Act of 1976 would suggest that data stored in RAM is not a “copy.” As noted above, a “copy” is defined as a material object in which a work is “fixed.” The statute defines a work to be “fixed in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.”¹¹ The legislative history states:

[T]he definition of “fixation” would exclude from the concept purely evanescent or transient reproductions such as those projected briefly on a screen, shown electronically on a television or other cathode ray tube, or captured momentarily in the “memory” of a computer.¹²

This language suggests that images of data temporarily stored in RAM do not constitute “copies.”¹³

Several cases, however, have held to the contrary. The leading case is MAI Systems Corp. v. Peak Computer, Inc.,¹⁴ which held that loading an operating system into RAM for maintenance purposes by an unlicensed third party maintenance organization created an illegal “copy” of the program fixed in RAM.¹⁵ When the MAI decision first came down, it was unclear whether that decision would support a legal principle that any storage of a copyrighted work in RAM, no matter how transiently, constituted a “copy” within the purview of copyright law, for the Ninth Circuit’s opinion in MAI seemed somewhat qualified. The court in MAI noted that the “copy” of the operating system was stored in RAM for several minutes (rather than only a few seconds). In addition, the court emphasized that while in RAM, output of the program was viewed by the user, which confirmed the conclusion that the RAM “copy” was capable of being perceived with the aid of a machine:

[B]y showing that Peak loads the software into the RAM and is then able to view the system error log and diagnose the problem with the computer, MAI has adequately shown that the representation created in the RAM is “sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.”¹⁶

¹¹ 17 U.S.C. § 101 (definition of “fixed in a tangible medium of expression”).

¹² H.R. Rep. No. 94-1476, at 53 (1976), *reprinted in* U.S.C.C.A.N. 5659, 5666.

¹³ But see R. Nimmer, Information Law ¶ 4.02[2], at 4-6 (2001) (“This language refers to subject matter protection and not whether particular acts create an infringing copy. The exclusion of transient works refers to the work itself, not a copy. It presumes that there was no copy of the work other than the transient display or memory.”)

¹⁴ 991 F.2d 511 (9th Cir. 1993), cert. dismissed, 114 S. Ct. 672 (1994).

¹⁵ Id. at 518.

¹⁶ 991 F.2d at 518.

In addition, a decision from the Seventh Circuit handed down shortly after MAI, NLFC, Inc. v. Devcom Mid-Am., Inc.,¹⁷ although somewhat unclear on both the facts involved in the case and whether the court really understood the issue, contains language that may suggest that merely proving that the defendant has remotely accessed the plaintiff's software through a terminal emulation program is not sufficient to prove that a "copy" has been made.¹⁸ Moreover, an earlier Ninth Circuit decision in the case of Lewis Galoob Toys, Inc. v. Nintendo of America, Inc.,¹⁹ implied that an image of data stored in RAM may not qualify as a "copy." At issue in that case was whether a device that altered certain bytes of data of a video game "on the fly" as such information passed through RAM created an infringing derivative work. The court held that it did not, because although a derivative work need not be fixed, it must have some "form" or "permanence," which were lacking in the enhanced displays created by the device. The court stated, however, that even if a derivative work did have to be fixed, the changes in the displayed images wrought on the fly by the accused device did not constitute a fixation because the transitory images it created were not "embodied" in any form.

¹⁷ 45 F.3d 231 (7th Cir. 1995).

¹⁸ Id. at 236.

¹⁹ 964 F.2d 965 (9th Cir. 1992).

Notwithstanding these earlier decisions, however, a great many courts have now followed MAI,²⁰ and some earlier decisions also support its conclusion.²¹ Although the opinion in

²⁰ See, e.g., Jeehoon Park v. Skidmore, Owings & Merrill LLP, 2019 U.S. Dist. LEXIS 171566 at *20 (S.D.N.Y. Sept. 30, 2019) (copying within the scope of the Copyright Act occurs when a file is accessed from a computer's hard drive and loaded into RAM); Take-Two Interactive Software, Inc. v. Zipperer, 2018 U.S. Dist. LEXIS 151169 at *2 (S.D.N.Y. Aug. 16, 2018) (same); VBConversions LLC v. Gulf Coast Ventures, Inc., 2016 U.S. Dist. LEXIS 105760 at *11 (C.D. Cal. Aug. 10, 2016) (citing MAI for the proposition that copying for purposes of copyright law occurs when a computer program is transferred from a permanent storage device to a computer's RAM); Live Face on Web, LLC v. The Control Group Media, 150 F. Supp. 3d 489, 498 (E.D. Penn. 2015) (under MAI, a visitor to one of the defendants' web pages featuring the plaintiff's software would download a copy into his computer's RAM, thereby infringing the copyright on the software); Soc'y of Holy Transfiguration Monastery, Inc. v. Gregory, 689 F.3d 29, 55 (1st Cir. 2012) (a computer makes a copy of a program when it transfers the program from a third party's computer or other storage device into its own memory); Carson v. Verismart Software, 2012 U.S. Dist. LEXIS 4166 at *8-9 (N.D. Cal. Mar. 27, 2012) (pleading alleging that defendants were "using" plaintiff's software without authorization was sufficient to state a copyright claim because the software had to be loaded into RAM to run, which constitutes the making of a fixed copy under MAI); Costar Realty Information, Inc. v. Field, 2010 U.S. Dist. LEXIS 135016 at *19 (D. Md. Dec. 20, 2010) (copies of web pages stored automatically in a computer's cache or RAM upon a viewing of the web page fall within the definition of "copy"); DocMagic, Inc. v. Ellie Mae, Inc., 745 F. Supp. 2d 1148 (N.D. Cal. 2010) (unauthorized loading of software into RAM constitutes an act of copying and thus of infringement); Apple, Inc. v. Psystar Corp., 673 F. Supp. 2d 931, 935 (N.D. Cal. 2009) (turning on computers that loaded into RAM copies of Apple's Mac OS X operating system containing unauthorized modifications constitute direct infringement of Apple's reproduction right); Quantum Sys. Integrators, Inc. v. Sprint Nextel Corp., 2009 U.S. App. LEXIS 14766 at *18-19 (4th Cir. July 7, 2009) (loading of software into RAM from unauthorized copies on hard disk was sufficiently fixed for purposes of copyright infringement); SimplexGrinnell LP v. Integrated Sys. & Power, Inc., 2009 U.S. Dist. LEXIS 30657 at *42 (S.D.N.Y. Apr. 8, 2009) (embodiment requirement is satisfied when a program is loaded for use into a computer's RAM and the duration requirement is satisfied when the program remains in RAM for several minutes or until the computer is shut off); MDY Industries, LLC v. Blizzard Entertainment, Inc., 2008 U.S. Dist. LEXIS 53988 (D. Ariz. July 14, 2008) (under MAI, copying software into RAM constitutes making a "copy" within the purview of copyright law, so that if a person is not authorized by the copyright holder through a license or by law (e.g. Section 117) to copy the software to RAM, the person commits copyright infringement when using the software in an unauthorized way); Airframe Sys., Inc. v. Raytheon Co., 520 F. Supp. 2d 258, 267 (D. Mass. 2007), aff'd, 601 F.3d 9 (1st Cir. 2010) (with regard to software, an act of copying sufficient to violate the Copyright Act occurs each time the software is run); Ticketmaster L.L.C. v. RMG Technologies, Inc., 507 F. Supp. 2d 1096, 1005 (C.D. Cal. 2007) (copies of web pages stored in a computer's cache or RAM upon a viewing of the web page fall within the Copyright Act's definition of a "copy"); Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc., 2004 U.S. Dist. LEXIS 12391 at *11-12 (D. Mass. July 2, 2004) (unauthorized copying of a program into RAM for use of the program infringes the copyright in the program); Lowry's Reports, Inc. v. Legg Mason, Inc., 271 F. Supp. 2d 737, 745 (D. Md. 2003) ("Unauthorized electronic transmission of copyrighted text, from the memory of one computer into the memory of another, creates an infringing 'copy' under the Copyright Act."); Stenograph L.L.C. v. Bossard Assocs., 144 F.3d 96 (D.C. Cir. 1998) (holding that an infringing copy of a computer program was made when that program was loaded into RAM upon boot up and used for its principal purposes); Triad Sys. v. Southeastern Express Co., 64 F.3d 1330 (9th Cir. 1995), cert. denied, 116 S. Ct. 1015 (1996); Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc., 53 U.S.P.Q.2d 1425 (D. Utah 1999); Tiffany Design, Inc. v. Reno-Tahoe Specialty, Inc., 55 F. Supp. 1113, 1121 (D. Nev. 1999) ("the digitization or input of any copyrighted material, whether it be computer code or visual imagery, may support a finding of infringement notwithstanding only the briefest of existence in a computer's RAM"); Marobie-FL Inc. v. National Association of Fire Equipment Distributors, 45 U.S.P.Q.2d 1236 (N.D. Ill. 1997); Advanced Computer

one of these decisions suggests that only copies that exist for several minutes should constitute a “copy” within the purview of copyright law,²² the others appear not to focus on how transitorily an image may be stored in RAM in ruling that such an image constitutes a “copy” for purposes of copyright law.

One of these decisions, Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.,²³ was the first decision to focus on whether the act of browsing on the Internet involves the creation of “copies” that implicate the copyright owner’s rights. In that case, the court, citing the MAI decision, flatly stated, “When a person browses a website, and by so doing displays the [copyrighted material], a copy of the [copyrighted material] is made in the computer’s random access memory (RAM), to permit viewing of the material. And in making a copy, even a temporary one, the person who browsed infringes the copyright.”²⁴ This decision, although quite direct in its holding, appears to address only the final “copy” that is made in the RAM of a Web surfer’s computer in conjunction with viewing a Web page through a browser. It does not address the trickier issue of whether whole or partial interim copies made in RAM of node computers during the course of transmission through the Internet also constitute “copies” within the purview of a copyright owner’s copyright rights.

However, a 2004 decision from the Fourth Circuit, CoStar v. Loopnet,²⁵ held that transient copies made by an OSP acting merely as a conduit to transmit information at the instigation of others does not create fixed copies sufficient to make it a direct infringer of copyright. “While temporary electronic copies may be made in this transmission process, they would appear not to be ‘fixed’ in the sense that they are ‘of more than transitory duration,’ and the ISP therefore would not be a ‘copier’ to make it directly liable under the Copyright Act.”²⁶ The court drew a distinction between the final copy of a work made in the RAM of the ultimate user’s computer, and the transient copies made by an OSP in the course of transmitting such copies:

In concluding that an ISP has not itself fixed a copy in its system of more than transitory duration when it provides an Internet hosting service to its subscribers, we do not hold

Servs. v. MAI Sys., 845 F. Supp. 356 (E.D. Va. 1994); see also 2 M. Nimmer & D. Nimmer, Nimmer on Copyright § 8.08[A][1], at 8-114 (1999) (suggesting that RAM copies are fixed).

²¹ See Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 260 (5th Cir. 1988) (“the act of loading a program from a medium of storage into a computer’s memory creates a copy of the program”); Apple Computer, Inc. v. Formula Int’l, 594 F. Supp. 617, 621 (C.D. Cal. 1984) (noting that copying a program into RAM creates a fixation, albeit a temporary one); Telerate Sys. v. Caro, 8 U.S.P.Q.2d 1740 (S.D.N.Y. 1988) (holding that the receipt of data in a local computer constituted an infringing copy).

²² Advanced Computer Services v. MAI Systems, 845 F. Supp. 356, 363 (E.D. Va. 1994).

²³ 53 U.S.P.Q.2d 1425 (D. Utah 1999).

²⁴ Id. at 1428.

²⁵ 373 F.3d 544 (4th Cir. 2004).

²⁶ Id. at 551.

that a computer owner who downloads copyrighted software onto a computer cannot infringe the software's copyright. See, e.g., MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511, 518-19 (9th Cir. 1993). When the computer owner downloads copyrighted software, it possesses the software, which then functions in the service of the computer or its owner, and the copying is no longer of a transitory nature. See, e.g., Vault Corp. v. Quaid Software, Ltd., 847 F.2d 255, 260 (5th Cir. 1988). "Transitory duration" is thus both a qualitative and quantitative characterization. It is quantitative insofar as it describes the period during which the function occurs, and it is qualitative in the sense that it describes the status of transition. Thus, when the copyrighted software is downloaded onto the computer, because it may be used to serve the computer or the computer owner, it no longer remains transitory. This, however, is unlike an ISP, which provides a system that automatically receives a subscriber's infringing material and transmits it to the Internet at the instigation of the subscriber.²⁷

A 2008 decision of the Second Circuit, The Cartoon Network LP v. CSC Holdings, Inc.,²⁸ addressed the issue of RAM copying in considerable detail, ruling that buffer copies in RAM made by Cablevision Systems Corp. in the course of converting channels of cable programming from the head end feed into a format suitable for storage of individual programs by a network digital video recording service upon customer demand were not fixed for sufficient duration to constitute "copies."²⁹ Cablevision made the buffer copies in conjunction with offering its "Remote Storage" Digital Video Recorder (RS-DVR) service that enabled Cablevision customers to record copies of particular programs, like a normal DVR, but to store the recorded programs on Cablevision's servers rather than on a DVR device at their homes. Cablevision created buffer copies, one small piece at a time, of the head end programming in two buffers – a primary ingest buffer and a Broadband Media Router (BMR) buffer – even if no customer requested that a copy of particular programming be stored on its behalf in the RS-DVR service. The primary ingest buffer held no more than 0.1 seconds of each incoming channel's programming at any moment. The data buffer in the BMR held no more than 1.2 seconds of programming at any time. The plaintiffs argued that these buffer copies made Cablevision a direct infringer of their copyrights.³⁰

The lower court found Cablevision a direct infringer largely in reliance on MAI and cases following it.³¹ The Second Circuit, however, reversed. The court noted that to satisfy the statutory definition of "copies," two requirements must be met – an "embodiment" requirement (embodiment in a tangible medium from which it can be perceived or reproduced) and a "duration" requirement (embodiment for a period of more than transitory duration). The

²⁷ Id.

²⁸ 536 F.3d 121 (2d Cir. 2008), cert. denied sub nom. CNN, Inc. v. CSC Holdings, Inc., 557 U.S. 946 (2009).

²⁹ Id. at 129-30.

³⁰ Id. at 123-24, 127.

³¹ Twentieth Century Fox Film Corp. v. Cablevision Sys. Corp., 478 F. Supp. 2d 607, 621-22 (S.D.N.Y. 2007).

Second Circuit found that the district court had mistakenly limited its analysis to the embodiment requirement, and that its reliance on MAI and cases following it was misplaced.³²

In general, those cases conclude that an alleged copy is fixed without addressing the duration requirement; it does not follow, however, that those cases assume, much less establish, that such a requirement does not exist. Indeed, the duration requirement, by itself, was not at issue in *MAI Systems* and its progeny.... Accordingly, we construe *MAI Systems* and its progeny as holding that loading a program into a computer's RAM *can* result in copying that program. We do not read *MAI Systems* as holding that, as a matter of law, loading a program into a form of RAM *always* results in copying.³³

Turning to the facts of the case at hand, the Second Circuit ruled that, although the embodiment requirement was satisfied by the buffers because the copyrighted works could be copied from them,³⁴ the duration requirement had not been satisfied. The court noted that no bit of data remained in any buffer for more than a fleeting 1.2 seconds, unlike the data in cases like MAI, which remained embodied in the computer's RAM until the user turned the computer off.³⁵ "While our inquiry is necessarily fact-specific, and other factors not present here may alter the duration analysis significantly, these facts strongly suggest that the works in this case are embodied in the buffer for only a 'transitory' period, thus failing the duration requirement."³⁶ Accordingly, the acts of buffering in the operation the RS-DVR did not create "copies" for which Cablevision could have direct liability.³⁷

The court in Costar Realty Information, Inc. v. Field³⁸ ruled that an allegation that the defendant accessed a password-protected database without authorization, which contained the plaintiff's copyrighted photographic images, raised a genuine dispute of material fact as to whether the defendant engaged in direct copyright infringement when he viewed the copyrighted work on a website that he did not have proper authorization to enter.³⁹ Citing the Intellectual Reserve case, the court ruled that "simply browsing a website that contains copyrighted material is sufficient to constitute copyright infringement because a copy of the

³² Cartoon Network, 536 F.3d 121 at 127.

³³ Id.

³⁴ Id. at 129. "The result might be different if only a single second of a much longer work was placed in the buffer in isolation. In such a situation, it might be reasonable to conclude that only a minuscule portion of a work, rather than 'a work' was embodied in the buffer. Here, however, where every second of an entire work is placed, one second at a time, in the buffer, we conclude that the work is embodied in the buffer." Id.

³⁵ Id.

³⁶ Id.

³⁷ Id. at 130.

³⁸ 2010 U.S. Dist. LEXIS 86567 (D. Md. Aug. 23, 2010).

³⁹ Id. at *37-38.

work is made in the computer's RAM to enable the images to display on the computer monitor."⁴⁰

3. The WIPO Treaties & the European Copyright Directive Are Unclear With Respect to Interim "Copies"

The language of two copyright treaties adopted during 1996 by the World Intellectual Property Organization (WIPO)⁴¹ leaves open the issue of whether transitory images of data stored in RAM constitute "copies."⁴²

(a) Introduction to the WIPO Treaties & the European Copyright Directive

The WIPO treaties were adopted as a result of the Diplomatic Conference on Certain Copyright and Neighboring Rights Questions hosted by WIPO in Geneva on December 2-20, 1996. More than 700 delegates from approximately 160 countries attended this Conference, which was aimed at tightening international copyright law to respond to issues arising from worldwide use of the Internet. The Conference was also designed to bring existing legislation on copyrights more in line with the provisions of the Trade Related Intellectual Property (TRIPS) sections of the Uruguay Round trade agreement, which in 1994 set up the World Trade Organization (WTO).⁴³

Three new treaties were considered, only two of which were adopted: the "WIPO Copyright Treaty" and the "WIPO Performances and Phonograms Treaty."⁴⁴ The WIPO Copyright Treaty strengthens the Berne Convention for the Protection of Literary and Artistic Works (the "Berne Convention"),⁴⁵ established in 1886, which was the first international copyright treaty. The WIPO Performances and Phonograms Treaty strengthens the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations, completed in Rome in 1961 (the "Rome Convention").⁴⁶

⁴⁰ *Id.* at *38.

⁴¹ WIPO is a United Nations organization which handles questions of copyrights and trademarks.

⁴² The treaties enter into force three months after 30 instruments of ratification or accession by member States have been deposited with the Director General of WIPO.

⁴³ Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, Legal Instruments – Results of the Uruguay Round vol. 31; 33 I.L.M. 81 (1994).

⁴⁴ The proposed WIPO Treaty on Intellectual Property in Respect of Databases generated huge controversy, and was not adopted at the Conference. "WIPO Delegates Agree on Two Treaties," 2 *BNA's Electronic Info. Pol'y & L. Rep.* 22, 22 (1997).

⁴⁵ Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, 828 U.N.T.S. 221.

⁴⁶ International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations, Oct. 26, 1961, 496 U.N.T.X. 43.

Each of the treaties required 30 nations to accede to it before it would enter into force. On Dec. 5, 2001, Gabon became the 30th nation to accede to the WIPO Copyright Treaty, and on Feb. 20, 2002, Honduras became the 30th nation to accede to the WIPO Performances and Phonograms Treaty. Accordingly, each of those treaties entered into force ninety days thereafter, on March 6, 2002 and May 20, 2002, respectively.⁴⁷ The treaties are not self-executing under United States law, and implementing legislation will have to be passed by Congress.

The two adopted treaties will effect important substantive changes in international copyright law that have potentially far reaching implications for the Internet, and the relevant provisions of these treaties will be discussed throughout this paper. The legislative history to the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty took the form of several “Agreed Statements.” Under the Vienna Convention, an Agreed Statement is evidence of the scope and meaning of the treaty language.⁴⁸ Relevant portions of the Agreed Statements will also be discussed in this paper.

Each of the signatories to the WIPO treaties was required to adopt implementing legislation to conform to the requirements of the treaties. The scope of legislation required in any particular country depends upon the substantive extent of that country’s copyright law existing at the time of the treaty, as well the country’s own views concerning whether its existing laws already conform to the requirements of the treaties. As discussed in detail below, WIPO implementation legislation in the United States took a largely minimalist view of the changes to United States copyright law required to conform to the WIPO treaties. It is curious that all the implementing legislation introduced in Congress implicitly took the position that U.S. law already contains most of the rights required under the WIPO treaties, in view of the fact that, as analyzed below, much of the language describing mandatory copyright rights in the WIPO treaties appears to go beyond the correlative rights in current United States law or to set up new rights entirely. The possibility that other countries would adopt legislation implementing the WIPO treaty rights in their seemingly broader form raises the prospect of varying scopes of rights in different countries, a situation that the WIPO treaties were intended to avoid in the first place.⁴⁹

In contrast to the United States implementing legislation, the European Commission’s “European Copyright Directive on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society”⁵⁰ to update and harmonize member state copyright laws

⁴⁷ “WIPO Copyright Treaty Enters Into Force As Gabon Becomes 30th Nation to Accede,” *BNA’s Electronic Commerce & Law Report* (Dec. 12, 2001) at 1224; “U.N. Announces Music Piracy Pact” (Feb. 21, 2002), available as of Feb. 21, 2002 at <http://news.com.com/2100-1023-842169.html>.

⁴⁸ Vienna Convention on the Law of Treaties, May 23, 1969, art. 31(2), 1155 U.N.T.S. 331.

⁴⁹ WIPO Copyright Treaty, Preamble, at 4; WIPO Performances and Phonograms Treaty, Preamble, at 22.

⁵⁰ The text of the European Copyright Directive may be found at http://europa.eu.int/servlet/portail/RenderServlet?search=DocNumber&lg=en&nb_docs=25&domain=Legislative&coll=&in_force=NO&an_doc=2001&nu_doc=29&type_doc=Directive (available as of January 1, 2002).

(which will be referred to herein as the “European Copyright Directive”) seems to take a more expansive view, although individual member states are free to interpret the extent to which their own copyright laws already conform to the dictates of the European Copyright Directive in adopting legislation in response to it.⁵¹ The WIPO implementation legislation in the United States and the European Copyright Directive will be discussed at length throughout this paper as they relate to the various issues treated herein.

(b) The WIPO Copyright Treaty

Article 7 of an earlier draft of the WIPO Copyright Treaty would apparently have adopted the approach of MAI to the question of whether RAM copies fall within the reproduction right of the copyright holder.⁵² The proposed Article 7(1) provided:

⁵¹ The European Copyright Directive was first circulated for comments among European legal experts. It was then officially published at the end of 1997 for a more public debate of its provisions. The European Parliament approved a final draft of the Directive on February 14, 2001. The European Commission, acting through the European Union ministers, accepted the final draft of the Directive on April 9, 2001.

⁵² The WIPO Copyright Treaty contains a number of important provisions relevant to the Internet that are not discussed elsewhere in this paper. Article 2 codifies the idea/expression dichotomy of copyright law: “Copyright protection extends to expressions and not to ideas, procedures, methods of operation or mathematical concepts as such.” Article 4 expressly extends copyright protection to computer programs in all forms as literary works: “Computer programs are protected as literary works within the meaning of Article 2 of the Berne Convention. Such protection applies to computer programs, whatever may be the mode or form of their expression.”

Article 5 adopts the approach of the Supreme Court’s decision in Feist Publications, Inc. v. Rural Telephone Serv., 499 U.S. 340 (1991), which held that only the selection or arrangement of a compilation of facts such as a database, and not the facts themselves, can be protected under copyright. Article 5 provides: “Compilations of data or other material, in any form, which by reason of the selection or arrangement of their contents constitute intellectual creations, are protected as such. This protection does not extend to the data or the material itself and is without prejudice to any copyright subsisting in the data or material contained in the compilation.” The proposed WIPO Treaty on Intellectual Property in Respect of Databases would have extended protection to the information itself in a database where such database was the fruit of substantial labor to compile. Basic Proposal for the Substantive Provisions of the Treaty on Intellectual Property in Respect of Databases to be Considered by the Diplomatic Conference, art. 1(1), WIPO Doc. CRNR/DC/6 (Aug. 30, 1996) <www.wipo.org/eng/diplconf/6dc_all.htm>. The controversy generated by this Treaty precluded its adoption by WIPO.

Article 7(1) provides that authors of computer programs, cinematographic works, and works embodied in phonograms shall enjoy the exclusive right of authorizing commercial rental to the public of the originals or copies of their works. Under Article 7(2), this rental right does not apply “in the case of computer programs where the program itself is not the essential object of the rental” or “in the case of cinematographic works, unless such commercial rental has led to widespread copying of such works materially impairing the exclusive right of reproduction.” The Agreed Statement for Articles 6 and 7 notes that the expressions “copies” and “original and copies,” being subject to the right of rental, “refer exclusively to fixed copies that can be put into circulation as tangible copies.”

Article 6 of an earlier draft of the treaty would have required Contracting Parties to abolish non-voluntary broadcasting licenses within seven years of ratifying or acceding to the Treaty. This Article was deleted in the final adopted version.

(1) The exclusive right accorded to authors of literary and artistic works in Article 9(1) of the Berne Convention of authorizing the reproduction of their works, in any manner or form, includes direct and indirect reproduction of their works, whether permanent or temporary.

The reference to “temporary” reproductions would have seemed to cover copies in RAM. The reference to “indirect” reproductions, particularly when coupled with the inclusion of “temporary” reproductions, might have been broad enough to cover interim, partial reproductions in RAM in the course of transmission of a work through the Internet, as well as complete copies of a work made in RAM and/or on a hard disk at the receiving computer.

In addition, proposed Article 7(2) of the treaty seemed to recognize the possibility that the language of Article 7(1) might be read to cover interim, partial reproductions during transmission, for it would have allowed signatory members (referred to as “Contracting Parties” in the treaty) to limit the right of reproduction in those instances:

(2) Subject to the conditions under, and without prejudice to the scope of applicability of, Article 9(2) of the Berne Convention, it shall be a matter for legislation in Contracting Parties to limit the right of reproduction in cases where a temporary reproduction has the sole purpose of making the work perceptible or where a temporary reproduction is of a transient or incidental nature, provided that such reproduction takes place in the course of use of the work that is authorized by the author or permitted by law in accordance with the Berne Convention and this Treaty.⁵³

⁵³ Although this provision apparently was designed to ameliorate the potential mischief that might result from deeming all interim copies of a work in the course of transmission to be within the copyright owner’s rights, it suffered from a number of potential problems. First, it would have left the issue up to the individual Contracting Parties whether to legislate exemptions. Thus, some Contracting Parties could have legislated such exemptions, while others did not, and the scope of the exemptions could have varied from country to country. As a result, whether interim copies during the course of transmission constitute infringement could have turned on the countries through which the transmission path passes, which is arbitrary under the current transmission technology of the Internet.

Second, Article 7(2) stated that the exemptions would apply only to transient or incidental reproductions taking place in the course of an authorized use of a work. Thus, if the transmission *itself* is unauthorized, the exemptions would not have applied, and there could still have been potential liability for the interim reproductions. Yet the operators of the node computers in which the interim copies are made would have no way of knowing whether any particular packet passing through the node is part of an authorized transmission. Article 7(2) therefore was flawed.

Article 10(1) of the adopted version affords a more generic vehicle for the adoption of exemptions or exceptions to rights conferred in the Treaty: “Contracting Parties may, in their national legislation, provide for limitations of or exceptions to the rights granted to authors of literary and artistic works under this Treaty to an extent consistent with exceptions or limitations provided for in the Berne Convention in certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author.”

The proposed Article 7, and the subject of interim transmission copies in general, generated a lot of controversy at the Conference. Telecommunications companies and Internet providers particularly objected to Article 7 because they feared that protection for temporary copying would impose liability for the interim copying that inherently occurs in computer networks. On the other hand, content providers such as the software, publishing and sound recording industries, opposed any open-ended approach that would permit all temporary copying.⁵⁴

To resolve the controversy, the proposed Article 7 was ultimately simply deleted entirely from the adopted version of the treaty.⁵⁵ The Agreed Statement pertaining to the right of reproduction (Previous Article 7) provides:

The reproduction right, as set out in Article 9 of the Berne Convention, and the exceptions permitted thereunder,⁵⁶ fully apply in the digital environment, in particular to the use of works in digital form. It is understood that the storage of a protected work in digital form in an electronic medium constitutes a reproduction within the meaning of Article 9 of the Berne Convention.

The Assistant Secretary of Commerce and Commissioner of Patents and Trademarks at the time, Bruce Lehman, who headed the U.S. delegation to the Conference, stated at the end of the Conference that the Agreed Statement was intended to make clear that the reproduction right includes the right to make digital copies, but also that certain copying, e.g., for temporary digital storage, will be permitted. Commissioner Lehman further expressed the view that the treaty language is broad enough to permit domestic legislation that would remove any liability on the part of network providers where the copying is simply the result of their functioning as a conduit for network services.⁵⁷ However, the Agreed Statement itself does nothing more than reference Article 9 of the Berne Convention, which of course was adopted long before digital copies were an issue under copyright law, and makes no explicit reference to “temporary digital storage.” In addition, the phrase “storage of a protected work in digital form in an electronic

The requirement that exceptions “not unreasonably prejudice the legitimate interests of the author” provides little guidance as to where the boundaries should lie around exceptions that Contracting Parties may wish to adopt in implementing legislation. The Agreed Statement concerning Article 10 does nothing to clarify the uncertainty: “It is understood that the provisions of Article 10 permit Contracting Parties to carry forward and appropriately extend into the digital environment limitations and exceptions in their national laws which have been considered acceptable under the Berne Convention. Similarly, these provisions should be understood to permit Contracting Parties to devise new exceptions and limitations that are appropriate in the digital network environment.”

⁵⁴ “WIPO Delegates Agree on Two Treaties,” 2 *BNA’s Electronic Info. Pol’y & L. Rep.* 22, 22 (1997).

⁵⁵ *Id.*

⁵⁶ Article 9(2) of the Berne Convention provides, “It shall be a matter for legislation in the countries of the Union to permit the reproduction of such works in certain special cases, provided that such reproduction does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author.”

⁵⁷ “WIPO Delegates Agree on Two Treaties,” 2 *BNA’s Electronic Info. Pol’y & L. Rep.* 22, 22-23 (1997).

medium” could potentially include temporary digital storage in a node computer during transmission. It is therefore difficult to agree with Commissioner Lehman that the Agreed Statement makes anything “clear.”

Rather, the Agreed Statement seems to leave virtually open ended the question of whether temporary images in RAM will be treated as falling within the copyright owner’s right of reproduction. The uncertainty surrounding the scope of the reproduction right in a digital environment that, at least early on, seemed to divide U.S. courts therefore appears destined to replicate itself in the international arena. The uncertainty is heightened by the fact that Article 9 of the Berne Convention allows signatories to adopt certain exceptions to the reproduction right, raising the prospect of inconsistent exceptions being adopted from country to country. As a result, whether interim copies made during the course of transmission constitute infringement may turn on the countries through which the transmission path passes, which is arbitrary under the current transmission technology of the Internet. The issue ignited debate in the United States in connection with the federal legislation to implement the treaty.

(c) The WIPO Performances and Phonograms Treaty

Curiously, despite the focus on and ultimate removal of the proposed Article 7 of the WIPO Copyright Treaty, Article 7 as adopted in the WIPO Performances and Phonograms Treaty appears to come closer to adopting the approach of MAI. Article 7 gives performers the exclusive right of “authorizing the direct or indirect reproduction of their performances fixed in phonograms” (emphasis added). As originally proposed, Article 7 contained language even closer to the MAI logic, for it expressed the reproduction right of performers as one of “authorizing the direct or indirect reproduction, whether permanent or temporary, of their performances fixed in phonograms” (emphasis added). The use of the phrase “permanent or temporary” would more strongly have suggested that temporary interim reproductions of performances would be within the performer’s right of reproduction.

In addition, Article 7(2) in an earlier draft was also deleted, which made reference to transient copies as follows:

Subject to the conditions under, and without prejudice to the scope of applicability of, Article 19(2), it shall be a matter for legislation in Contracting Parties to limit the right of reproduction in cases where a temporary reproduction has the sole purpose of making the fixed performance perceptible or where a temporary reproduction is of a transient or incidental nature, provided that such reproduction takes place in the course of use of the fixed performance that is authorized by the performer or permitted by law in accordance with this Treaty.

The Agreed Statement that was issued with respect to the right of reproduction in the WIPO Performances and Phonograms Treaty is very similar to the Agreed Statement on the same subject that was issued with the WIPO Copyright Treaty. The Agreed Statement issued with the WIPO Performances and Phonograms Treaty provides:

The reproduction right, as set out in Articles 7 and 11, and the exceptions permitted thereunder through Article 16, fully apply in the digital environment, in particular to the use of performances and phonograms in digital form. It is understood that the storage of a protected performance or phonogram in digital form in an electronic medium constitutes a reproduction within the meaning of these Articles.

Thus, the Agreed Statement for the WIPO Performances and Phonograms Treaty contains the same ambiguities noted above with respect to the Agreed Statement for the WIPO Copyright Treaty.

Similar to Article 7, Article 11 gives producers of phonograms the “exclusive right of authorizing the direct or indirect reproduction of their phonograms, in any manner or form.” As in the case of Article 7, an earlier proposed version of Article 11 contained the phrase “whether permanent or temporary,” but this phrase was deleted in the final adopted version.⁵⁸

Both Articles 7 and 11 define the rights recited therein in terms of “phonograms.” “Phonogram” is defined in Article 2(b) as any “fixation” of the sounds of a performance or of other sounds other than incorporated in a cinematographic or other audiovisual work.

“Fixation” is defined broadly in Article 2(c) as “the embodiment of sounds or the representations thereof, from which they can be perceived, reproduced or communicated through a device.” Storage in RAM would seem to satisfy this definition of fixation. Thus, any unauthorized transmission of a performance, or of the sounds embodied in a phonogram fixing such performance, to RAM memory would potentially violate the rights of both the owner of the performance and of the phonogram.⁵⁹

⁵⁸ Article 11(2) in an earlier draft, similar to the proposed and later deleted Article 7(2), was also deleted. Article 11(2) would have provided: “Subject to the conditions under, and without prejudice to the scope of applicability of, Article 19(2), it shall be a matter for legislation in Contracting Parties to limit the right of reproduction in cases where a temporary reproduction has the sole purpose of making the phonogram audible or where a temporary reproduction is of a transient or incidental nature, provided that such reproduction takes place in the course of use of the phonogram that is authorized by the producer of the phonogram or permitted by law in accordance with this Treaty.”

⁵⁹ The WIPO Performances and Phonograms Treaty contains a number of important provisions relevant to the Internet that are not discussed elsewhere in this paper. Article 4 requires Contracting Parties to afford national treatment to nationals of other Contracting Parties. Article 5(1) affords moral rights to performers: “Independently of a performer’s economic rights, and even after the transfer of those rights, the performer shall, as regards his live aural performances or performances fixed in phonograms, have the right to claim to be identified as the performer of his performances, except where omission is dictated by the manner of the use of the performance, and to object to any distortion, mutilation or other modification of his performances that would be prejudicial to his reputation.” A proposed Article 5(4), which was deleted in the final version, would have allowed any Contracting Party to declare in a notification deposited with the Director General of WIPO that it will not apply the provisions of Article 5.

Article 6 grants performers the exclusive right of authorizing the broadcasting and communication to the public of their unfixed performances (except where the performance is already a broadcast performance) and the

Thus, the WIPO Performances and Phonograms Treaty replicates the same uncertainty as the WIPO Copyright Treaty with respect to the issue of whether transient “copies” of performances and phonograms will fall within the copyright owner’s right of reproduction.⁶⁰ Indeed, the definition of the right of reproduction in Article 7 and Article 11 to include “direct or indirect” reproductions, together with the broad definition of “fixation” in Article 2(c), arguably adopt an approach that is closer to the MAI decision than the WIPO Copyright Treaty.

4. The Requirement of Volition for Direct Liability

Even assuming the rationale of the MAI case and the provisions of the WIPO Treaties are applied to deem all reproductions during transmission of a work through the Internet to be “copies” within the copyright owner’s rights, a difficult issue arises as to who should be responsible for the making of such copies. Multiple actors may be potentially connected with a particular copy or copies of a work on the Internet, such as a work posted to a bulletin board service (BBS) – the original poster of the work, the BBS operator, the Online Service Provider (OSP) through which the BBS is offered, a user downloading a copy of the work from the BBS, and perhaps the operators of node computers through which a copy of the work may pass during the course of such downloading. Which one or more of these actors should be deemed to have made the copy or copies?

The most difficult aspect of the issue of which actors should be liable for copies made in the course of the downloading, viewing or other transmission of a work through the Internet

fixation of their unfixed performances. Articles 9 and 13 grant performers and producers of phonograms, respectively, the exclusive right of authorizing the commercial rental to the public of the original and copies of their performances fixed in phonograms and of their phonograms.

Article 15 provides, “Performers and producers of phonograms shall enjoy the right to a single equitable remuneration for the direct or indirect use of phonograms published for commercial purposes for broadcasting or for any communication to the public.” The Agreed Statement for Article 15 provides: “It is understood that Article 15 does not represent a complete resolution of the level of rights of broadcasting and communication to the public that should be enjoyed by performers and phonogram producers in the digital age. Delegations were unable to achieve consensus on differing proposals for aspects of exclusivity to be provided in certain circumstances or for rights to be provided without the possibility of reservations, and have therefore left the issue to future resolution.”

Under Article 17(1), the term of protection to be granted to performers under the Treaty is at least 50 years from the end of the year in which the performance was fixed in a phonogram. Under Article 17(2), the term of protection to be granted to producers of phonograms under the Treaty is at least 50 years from the end of the year in which the phonogram was published, or failing such publication within 50 years from fixation of the phonogram, 50 years from the end of the year in which the fixation was made.

⁶⁰ Article 16 affords a generic vehicle for the adoption of exemptions or exceptions to rights conferred in the Treaty. Article 16(1) provides that “Contracting Parties may, in their national legislation, provide for the same kinds of limitations or exceptions with regard to the protection of performers and producers of phonograms as they provide for in their national legislation, in connection with the protection of copyright in literary and artistic works.” Article 16(2) provides, however, similar to the WIPO Copyright Treaty, that “Contracting Parties shall confine any limitations of or exceptions to rights provided for in this Treaty to certain special cases which do not conflict with a normal exploitation of the phonogram and do not unreasonably prejudice the legitimate interests of the performer or of the producer of phonograms.”

stems from the fact that many such copies will typically be made *automatically*. For example, “copies” of the work (in whole or in part) will automatically be made in the RAM (and possibly in temporary hard disk storage) of each interim node computer within the transmission path of the work through the Internet. And the modems on the initiating and receiving ends of the transmission will buffer the data to be transmitted. Internet search engine services may use “spiders” to “crawl” through the Internet and make copies in RAM of materials on websites in the course of creating an index of that material.

Should a volitional act be required on the part of a third party to be liable for a copy made during transmission? If so, is a *direct* volitional act to cause the copy to be made required (as in the case of the original poster or the ultimate recipient of the copy), or is it sufficient if there was a volitional act in setting up the automatic process that ultimately causes the copy to be made (as in the case of the BBS operator, the OSP or the search engine service)? In view of the fact that copyright law has traditionally imposed a standard of strict liability for infringement,⁶¹ one could argue that a direct volitional act may not be required.⁶²

In addition to copies made automatically on the Internet, many infringing copies may be made *innocently*. For example, one may innocently receive an e-mail message that infringes the copyright rights of another and print that message out. Or one may innocently encounter (and copy into the RAM of one’s computer or print out) infringing material in the course of browsing.

Several cases have addressed the issue of direct liability on the part of OSPs, BBS operators, and others for infringement of the reproduction right by users of the service, and in particular how much of a volitional act is required for direct infringement liability:⁶³

(a) The Netcom Case

The well-known case of Religious Technology Center v. Netcom On-Line Communication Services⁶⁴ refused to impose direct infringement liability on an OSP for copies made through its service, at least where the OSP had no knowledge of such infringements. In that case the plaintiffs sought to hold liable the OSP (Netcom) and the operator of a BBS which gained its Internet access through the OSP for postings of the plaintiffs’ copyrighted works on the bulletin board. The works in question were posted by an individual named Erlich⁶⁵ to the BBS’s

⁶¹ Religious Technology Center v. Netcom On-Line Communications Servs., 907 F. Supp. 1361, 1367 & n.10 (N.D. Cal. 1995); R. Nimmer, Information Law ¶ 4.06, at 4-25 (2001). Intent can, however, affect statutory damages to be awarded to the plaintiff. Netcom, 907 F. Supp. at 1367.

⁶² But cf. R. Nimmer, Information Law ¶ 4.06, at S4-50 (2001 Cum. Supp. No. 2) (“Although copyright is a strict liability statute, there should be some [sort] of volition or causation which is lacking where a defendant’s system is merely used to create a copy by a third party.”).

⁶³ See also cases discussed in Section III.C.1 below pertaining to direct liability of online service providers.

⁶⁴ 907 F. Supp. 1361 (N.D. Cal. 1995).

⁶⁵ In an earlier order, the court had entered a preliminary injunction against Erlich himself.

computer for use through Usenet.⁶⁶ The BBS's computer automatically briefly stored them. The OSP then automatically copied the posted works onto its computer and onto other computers on the Usenet. In accordance with usual Usenet procedures, Usenet servers maintained the posted works for a short period of time – eleven days on Netcom's computer and three days on the BBS's computer.⁶⁷ The OSP neither created nor controlled the content of the information available to its subscribers, nor did it take any action after being told by the plaintiffs that Erlich had posted infringing messages through its system.⁶⁸

The court cast the issue of direct liability as “whether possessors of computers are liable for incidental copies automatically made on their computers using their software as part of a process initiated by a third party.”⁶⁹ The court distinguished MAI, noting that “unlike MAI, the mere fact that Netcom's system incidentally makes temporary copies of plaintiffs' works does not mean that Netcom has caused the copying. The court believes that Netcom's act of designing or implementing a system that automatically and uniformly creates temporary copies of all data sent through it is not unlike that of the owner of a copying machine who lets the public make copies with it.”⁷⁰ The court held that, absent any volitional act on the part of the OSP or the BBS operator other than the initial setting up of the system, the plaintiffs' theory of liability, carried to its natural extreme, would lead to unreasonable liability:

Although copyright is a strict liability statute, there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party.⁷¹

Accordingly, the court refused to hold the OSP liable for direct infringement. The court also refused to hold the BBS operator liable for direct infringement. “[T]his court holds that the storage on a defendant's system of infringing copies and retransmission to other servers is not a direct infringement by the BBS operator of the exclusive right to *reproduce* the work where such copies are uploaded by an infringing user.”⁷² The court further held that the warning of the presence of infringing material the plaintiffs had given did not alter the outcome with respect to direct infringement liability:

⁶⁶ The Usenet is “a worldwide community of electronic BBSs that is closely associated with the Internet and with the Internet community. The messages in Usenet are organized into thousands of topical groups, or ‘Newsgroups’ As a Usenet user, you read and contribute (‘post’) to your local Usenet site. Each Usenet site distributes its users' postings to other Usenet sites based on various implicit and explicit configuration settings, and in turn receives postings from other sites.” Daniel P. Dern, *The Internet Guide for New Users* 196-97 (1994).

⁶⁷ Netcom, 907 F. Supp. at 1367.

⁶⁸ Id. at 1368.

⁶⁹ Id.

⁷⁰ Id. at 1369.

⁷¹ Id. at 1370.

⁷² Id. at 1370-71 (emphasis in original).

Whether a defendant makes a direct copy that constitutes infringement cannot depend on whether it received a warning to delete the message. This distinction may be relevant to contributory infringement, however, where knowledge is an element.⁷³

The result of the Netcom case with respect to liability for direct infringement for the transmission and intermediate storage of copyrighted materials by an OSP was codified in the first safe harbor for OSPs set forth in Section 512(a)(1) of the Digital Millennium Copyright Act,⁷⁴ discussed in detail in Section III.C below.

(b) The MAPHIA Case

Another well-known case, Sega Enterprises Ltd. v. MAPHIA,⁷⁵ adopted the logic of the Netcom case and refused to hold a BBS and its system operator directly liable for the uploading and downloading of unauthorized copies of Sega's video games, even though the defendants participated in encouraging the unauthorized copying, which was not true in Netcom. (As discussed below, the court did, however, find contributory liability.) The evidence established that the system operator had knowledge that the infringing activity was going on through the bulletin board, and indeed that he had specifically solicited the uploading of the games for downloading by users of the bulletin board.⁷⁶ The system operator also sold video game "copiers," known as "Super Magic Drives," through the MAPHIA BBS, which enabled subscribers to the BBS to play games which had been downloaded from the BBS.⁷⁷

In granting a motion by Sega seeking summary judgment and a permanent injunction, the court refused to impose direct liability for copyright infringement on the BBS and its system operator, Chad Sherman. The court cited the Netcom case for the proposition that, although copyright is a strict liability statute, there should be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party.⁷⁸ The court further stated:

While Sherman's actions in this case are more participatory than those of the defendants in Netcom, the Court finds Netcom persuasive. Sega has not shown that Sherman

⁷³ Id. at 1370.

⁷⁴ H.R. Rep. No. 105-551 Part 1, at 11, 24 (1998).

⁷⁵ 948 F. Supp. 923 (N.D. Cal. 1996).

⁷⁶ Id. at 928.

⁷⁷ Id. at 929. The Super Magic Drive consisted of a connector which plugged into the video game console, a receptacle which accepted video game cartridges, a main unit having a RAM to store games, and a floppy disk drive. "A MAPHIA BBS user can download video programs through his or her computer onto a floppy disk and make copies with his or her computer or play those game programs through the adaptor drive. To play a downloaded game, the user places the floppy disk into the video game copier. The user can choose the 'run program' option and run the video game program from the floppy disk without a video game cartridge. The adaptor drive also allows the user to copy the contents of a game cartridge onto a floppy disk." Id.

⁷⁸ Id. at 932.

himself uploaded or downloaded the files, or directly caused such uploading or downloading to occur. The most Sega has shown is that Sherman operated his BBS, that he knew infringing activity was occurring, and that he solicited others to upload games. However, whether Sherman knew his BBS users were infringing on Sega's copyright, or encouraged them to do so, has no bearing on whether Sherman directly caused the copying to occur. Furthermore, Sherman's actions as a BBS operator and copier seller are more appropriately analyzed under contributory or vicarious liability theories. Therefore, because Sega has not shown that Sherman directly caused the copying, Sherman cannot be liable for direct infringement.⁷⁹

(c) The Sabella Case

Similarly, in Sega Enterprises Ltd. v. Sabella,⁸⁰ the court refused to hold a BBS operator liable for direct infringement of the reproduction right where there was no evidence that the operator did any unauthorized copying herself. The defendant, Sabella, was the system operator of a BBS called "The Sewer Line," which contained a directory called "Genesis," into which were uploaded and downloaded infringing copies of Sega's video games by subscribers to the BBS. The defendant also sold copiers that enabled users to play Sega games directly from floppy disks without the need for a Sega game cartridge, and allowed purchasers of her copiers to download files from her BBS without charge for a certain time period.

⁷⁹ Id. (citations to Netcom omitted). An earlier opinion in the case, issued in conjunction with the granting of a preliminary injunction to Sega, although somewhat unclear in its holding, seemed to suggest that the defendants *could* be held liable for direct infringement, at least for the unauthorized copies being uploaded through the bulletin board, although not for the subsequent downloading of copies by user of the bulletin board. See Sega Enterprises Ltd. v. MAPHIA, 857 F. Supp. 679, 683 (N.D. Cal. 1994). The court in the later opinion, however, disavowed this interpretation of its earlier opinion. With respect to its earlier order granting a preliminary injunction, the court stated, "To the extent that order can be read to suggest that Sherman may be liable for direct copyright infringement, it is clarified and superseded by this order." Sega Enterprises Ltd. v. MAPHIA, 948 F. Supp. 923, 932 n.5 (N.D. Cal. 1996).

The court also rejected a fair use defense raised by Sherman. With respect to the first fair use factor, the purpose and character of the use, the court found that Sherman's activities in encouraging the uploading and downloading of Sega's games was clearly commercial. "Sherman intended to profit directly from the content of the information made available on his BBS because his copier customers could use the game files to play the games rather than purchase Sega game cartridges. This distinguishes Sherman from the Internet provider in Netcom who did not gain anything from the content of the information available to subscribers." Id. at 934.

With respect to the second fair use factor, the nature of the copyrighted work, the court noted that the Sega video games were for entertainment uses and involved fiction and fantasy, so that the second factor weighed against fair use. Id. The court found that the third factor, the extent of the work copied, weighed against fair use because BBS users copied virtually entire copyrighted works, and Sherman had not shown any public benefit or explanation for the complete copying. Id. at 935. Finally, the court found that the fourth factor, the effect of the use upon the market, also weighed against fair use. "Even if the users are only playing the games in their own homes and even if there are currently only a limited number of users that have copiers, unrestricted and widespread conduct of this sort would result in a substantial adverse impact on the market for the Sega games." Id.

⁸⁰ 1997 Copyr. Law. Dec. ¶ 27,648 (N.D. Cal. Dec. 18, 1996).

Although the court agreed that the defendant's activities were more participatory than those of the defendant in Netcom, the court nevertheless found the Netcom court's logic persuasive. "Sega has not shown that Sabella herself uploaded or downloaded the files, or directly caused such uploading or downloading to occur. The most Sega has shown is that Sabella should have known such activity was occurring, that she sold copiers that played games such as those on her BBS, and that she gave her copier customers downloading privileges on her BBS."⁸¹ Citing Netcom, the court concluded that "whether Sabella knew her BBS users were infringing on Sega's copyright or encouraged them to do so, has no bearing on whether Sabella directly caused the copying to occur."⁸²

The court did rule, however, that Sabella was liable for contributory infringement. The court cited the Ninth Circuit's holding in Fonovisa, Inc. v. Cherry Auction, Inc. that "providing the site and facilities for known infringing activity is sufficient to establish contributory liability."⁸³ The court noted that Sabella provided the BBS as a central depository site for the unauthorized copies of games, and allowed subsequent distribution of the games by user downloads. "She provided the facilities for copying the games by providing, monitoring, and operating the BBS software, hardware, and phone lines necessary for the users to upload and download games."⁸⁴ Accordingly, she was liable for contributory infringement under the Fonovisa standard.⁸⁵

The court went further, however, holding that even an alternative and higher standard of "substantial participation," Sabella was liable. "Sabella did more than provide the site and facilities for the known infringing conduct. She provided a road map on the BBS for easy identification of Sega games available for downloading."⁸⁶ The court also rejected Sabella's fair use defense, issued a permanent injunction against Sabella, and awarded Sega statutory damages of \$5,000 per infringed work.

In contrast to the preceding cases, several cases have held that where a defendant BBS operator has a more direct participation in the acts of infringement of its subscribers or users, there can be direct infringement liability for those acts:

⁸¹ Id. at 29,847-48.

⁸² Id. at 29,848.

⁸³ 76 F.3d 259, 264 (9th Cir. 1996).

⁸⁴ Sabella, 1997 Copyr. Law. Dec. ¶ 27,648 at 29,849.

⁸⁵ Another case applied the Fonovisa standard to hold the defendant Cyrix Corporation liable for contributory infringement for posting on its website some copyrighted applet software of the plaintiff from which it could be downloaded for use with the defendant's sound boards. "Cyrix is probably also contributorily liable because it encouraged and provided the resources for known infringing activity, i.e. the copying by others of the applet software that Cyrix made available on its website." Creative Labs, Inc. v. Cyrix Corp., 42 U.S.P.Q.2d 1872, 1875-76 (N.D. Cal. 1997).

⁸⁶ Sabella, 1997 Copyr. Law. Dec. ¶ 27,648 at 29,849.

(d) The Frena Case

Playboy Enterprises, Inc. v. Frena,⁸⁷ decided before Netcom, MAPHIA and Sabella, goes further than those cases and established liability for the acts of subscribers without a direct volitional act on the part of the operator. In that case, the court held the operator of a BBS, Frena, responsible for infringement of the rights of *distribution* and *display* (although curiously not the right of reproduction) with respect to the plaintiff's copyrighted photographs, which were distributed and displayed through the bulletin board by subscribers, despite evidence that the operator never himself uploaded any of the photographs onto the bulletin board and removed the photographs as soon as he was made aware of them.⁸⁸ "There is no dispute that Defendant Frena supplied a product containing unauthorized copies of a copyrighted work. It does not matter that Defendant Frena claims he did not make the copies [himself]." ⁸⁹ Although the case did not generate a finding of liability with respect to the right of reproduction, the court's logic with respect to finding infringement of the rights of distribution and display would seem to apply to the reproduction right as well.

The reach of Frena may be limited, however, because the BBS was apparently one devoted to photographs, much of it of adult subject matter, and subscribers routinely uploaded and downloaded images therefrom. Thus, the court may have viewed Frena as a more direct participant in the infringement, having set up a bulletin board that was devoted to the kind of activity that would foreseeably lead to infringement. The undisputed evidence of the presence on the bulletin board of the plaintiff's photographs, some of which had been edited to remove the plaintiff's trademarks and to add Frena's advertisements, was apparently evidence of sufficient involvement for the court to find direct infringement of the public distribution right. Similarly, Frena's selection of the infringing content for inclusion in the bulletin board was apparently sufficient involvement to find direct infringement of the public display right.⁹⁰

In addition, as discussed in detail below, the legislative history of the Digital Millennium Copyright Act, which contains a number of safe harbors that address the issue of OSP liability, states that it was intended to overrule the Frena case, at least to the extent Frena suggested that passive, automatic acts engaged in through a technological process initiated by another through the facilities of an OSP could constitute direct infringement on the part of the OSP.⁹¹ In a case decided in 2001, the Fourth Circuit held that the Digital Millennium Copyright Act had indeed

⁸⁷ 839 F. Supp. 1552 (M.D. Fla. 1993).

⁸⁸ Id. at 1554.

⁸⁹ Id. at 1556.

⁹⁰ K. Stuckey, Internet and Online Law § 6.10[2][a], at 6-80 (2013).

⁹¹ H.R. Rep. No. 105-551 Part 1, at 11 (1998).

overruled Frena “insofar as that case suggests that [passive, automatic acts engaged in through a technological process initiated by another] could constitute direct infringement.”⁹²

(e) The Webworld Case

In a case factually similar to Frena, a company operating a website was held directly liable for the posting of copyrighted material on its site which could be downloaded by subscribers. In Playboy Enterprises, Inc. v. Webworld, Inc.,⁹³ the defendant Webworld, Inc. operated a website called Neptics, which made adult images available to subscribers who paid \$11.95 per month. Over a period of several months, images became available through the Neptics website which were originally created by or for the plaintiff Playboy Enterprises, Inc.

The court rejected the defendant’s argument that it could not be held directly liable for infringement under the logic of the Netcom case. The court distinguished the Netcom case on the ground that Netcom did not create or control the content of the information available to its subscribers, but rather merely provided access to the Internet. In contrast, the court noted that Neptics was receiving payment selling the images it stored on its computers, and therefore was acting as more than merely an information conduit.⁹⁴

The defendant also argued that it could not be held liable for direct infringement because it had no control over the persons who posted the infringing images to the adult newsgroups from which Neptics obtained its material. The court rejected this argument: “While this may be true, Neptics surely has control over the images it chooses to sell on the Neptics’ website. Even the absence of the ability to exercise such control, however, is no defense to liability. If a business cannot be operated within the bounds of the Copyright Act, then perhaps the question of its legitimate existence needs to be addressed.”⁹⁵

⁹² ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 622 (4th Cir. 2001). A subsequent district court cited with approval the Fourth Circuit’s decision on this point. See Costar Group Inc. v. Loopnet, Inc., 164 F. Supp. 2d 688, 695-96 (D. Md. 2001), aff’d, 373 F.3d 544 (4th Cir. 2004).

⁹³ 968 F. Supp. 1171 (N.D. Tex. 1997).

⁹⁴ Id. at 1175.

⁹⁵ Id. The court also held that the principals of Webworld could be held vicariously liable for the infringements. Although the principals had no control over those responsible for originally uploading the infringing images onto the Internet sites from which Webworld drew its images, the principals had the right and ability to control what occurred on the Neptics website. The court ruled that the \$11.95 subscription fee gave the principals a sufficient direct financial benefit from the infringing activity to hold them vicariously liable. Id. at 1177.

The court made its rulings in the context of a motion for summary judgment by the plaintiff. The court granted summary judgment of infringement with respect to sixty-two copyrighted images, but denied summary judgment with respect to sixteen additional images because of the presence of material issues of fact. In a subsequent ruling, the court found the defendants directly and vicariously liable with respect to these sixteen additional images based on a similar legal analysis of liability. See Playboy Enterprises, Inc. v. Webworld, Inc., 45 U.S.P.Q.2d 1641 (N.D. Tex. 1997).

(f) The Sanfilippo Case

In Playboy Enterprises, Inc. v. Sanfilippo,⁹⁶ the court found the defendant operator of a website through which 7475 of the plaintiff's copyrighted images were available directly liable for infringement. The defendant admitted copying 16 files containing a great many of the images from a third party source onto his hard drive and CD-ROM. He also admitted that 11 other files containing such images were uploaded to his hard drive by a third party. The court found that, because the defendant had authorized the third party to upload such files to his site, the defendant was directly liable for such upload as a violation of the exclusive right under Section 106 of the copyright statute to "authorize" others to reproduce a copyrighted work. The court also found that the defendant had willfully infringed 1699 of the copyrighted images.

One of the most interesting aspects of the Sanfilippo case is the amount of damages the court awarded. The plaintiff sought statutory damages, and argued that a statutory damages award should be made for each individual image that was infringed. The defendant argued that, in awarding damages, the court should consider the fact that the copied images were taken from compilations and, therefore, an award should be made only with respect to each particular magazine's copyright from which the images were taken. The court rejected this argument and allowed a statutory damage award for each image on the grounds that each image had an independent economic value on its own, each image represented "a singular and copyrightable effort concerning a particular model, photographer, and location,"⁹⁷ and the defendant marketed each one of the images separately. The court awarded statutory damages of \$500 per image, for a total damage award of \$3,737,500.⁹⁸

(g) The Free Republic Case

Even where there is a direct volitional act on the part of a website operator in copying copyrighted material onto its site, difficult questions relating to First Amendment and fair use rights may arise, particularly where the Web is used to facilitate free ranging discussion among participants. For example, in 1998, the Los Angeles Times and The Washington Post filed a copyright infringement lawsuit against the operator of a website called the Free Republic. The site contained news stories from dozens of sources (including the plaintiffs), posted both by the operator of the site and its users, and users were allowed to attach comments to the stories.⁹⁹ The plaintiffs argued that, because verbatim complete copies of their news stories were often posted on the website, it was reducing traffic to their own websites on which the articles were posted, and was harming their ability to license their articles and to sell online copies of archived

⁹⁶ 1998 U.S. Dist. LEXIS 5125 (S.D. Cal. 1998).

⁹⁷ Id. at *18-19.

⁹⁸ The plaintiff requested an astronomical \$285,420,000 in statutory damages (\$20,000/image for 5776 images that were not willfully infringed, and \$100,000/image for 1699 images that were willfully infringed).

⁹⁹ Los Angeles Times v. Free Republic, 54 U.S.P.Q.2d 1453, 1455-56 (C.D. Cal. 2000).

articles.¹⁰⁰ The defendants raised defenses under the fair use doctrine and under the First Amendment.¹⁰¹ The defendants moved for summary judgment on all claims and the plaintiffs cross moved for summary judgment on the defendants' defense of fair use.

The court rejected the defendants' fair use argument and ruled that the defendants might be liable for infringement.¹⁰² The court ruled that the first fair use factor (purpose and character of the use) favored the plaintiffs, noting there was little transformative about copying the entirety or portions of the articles, since the articles on the defendants' site served the same purpose as that for which one would normally seek to obtain the original – for ready reference if and when websites visitors needed to look at it.¹⁰³ The court also rejected the addition of commentary to the articles as favoring the defendants under the first factor, noting that the first posting of an article to the site often contained little or no transforming commentary, and in most cases it was not necessary to copy verbatim the entire article in order for users to be able to comment on the article.¹⁰⁴ Finally, the court noted that the Free Republic site was a for-profit site, for which the copying enhanced the defendants' ability to solicit donations and generate goodwill for their website operation and other businesses of the website operator.¹⁰⁵

The second fair use factor (nature of the copyrighted work) favored the defendants, because the copied news articles were predominantly factual in nature.¹⁰⁶ The third fair use factor (amount and substantiality of the portion used in relation to the copyrighted work as a whole) favored the plaintiffs, because in many cases exact copies of the entire article were made and the court had previously found that copying of the entire article was not necessary to comment on it.¹⁰⁷ Finally, the fourth fair use factor (effect of the use on the potential market for or value of the copyrighted work) favored the plaintiffs, because the court found that the availability of complete copies of the articles on the Free Republic site fulfilled at least to some extent demand for the original works and diminished the plaintiffs' ability to sell and license their

¹⁰⁰ Id. at 1457.

¹⁰¹ Id. at 1454-55.

¹⁰² The court limited its opinion to the availability of the defenses on which the defendants had moved for summary judgment. The court stated it was expressing no opinion as to whether, "given that the 'copying' of news articles at issue in this case is to a large extent copying by third-party users," the plaintiffs could prove a claim against the defendants for copyright infringement. Id. at 1458.

¹⁰³ Id. at 1460-61.

¹⁰⁴ Id. at 1461 & 1463-64. The most telling fact on the latter point was that the Free Republic provided a hypertext link to *Jewish World Review's* website at its request, and asked that Free Republic visitors no longer copy the publication's articles verbatim. Id. at 1463.

¹⁰⁵ Id. at 1464-66.

¹⁰⁶ Id. at 1467.

¹⁰⁷ Id. at 1468.

articles.¹⁰⁸ On balance, then, the court concluded that the defendants could not establish a fair use defense.¹⁰⁹

The court also rejected the defendants' First Amendment defense on the ground that the defendants had failed to show that copying entire news articles was essential to convey the opinions and criticisms of visitors to the site. The court noted that visitors' critiques could be attached to a summary of the article, or Free Republic could have provided a link to the plaintiffs' websites where the articles could be found.¹¹⁰

The parties subsequently settled the case, pursuant to which the court entered a stipulated final judgment enjoining the defendants from copying, posting, uploading, downloading, distributing or archiving any of the plaintiffs' works, or encouraging others to do so, or operating any website or other online service that accomplished or permitted any of the foregoing, except as otherwise permitted by the plaintiffs in writing or by the fair use doctrine. The defendants agreed to pay \$1,000,000 in statutory damages for past infringing acts.¹¹¹

(h) The MP3.com Cases

In 2000, the Recording Industry Association of America, Inc. (RIAA), on behalf of 10 of its members, filed a complaint in federal court in the Southern District of New York for willful copyright infringement against MP3.com, based on MP3.com's new "My.MP3" service.¹¹² According to the complaint, this service allowed users to gain access through the Internet, and download digital copies of, commercial CDs, using one of two component services:

"Instant Listening Service" – Under this service, a user could place an order for a commercial CD through one of several online CD retailers cooperating with MP3.com, and then immediately have access to the song tracks on that CD stored on an MP3.com server, before arrival of the shipment of the physical CD ordered by the user.¹¹³

"Beam-it" – Under this service, a user could insert a commercial CD or a copy thereof (authorized or unauthorized) into his or her computer CD-ROM drive. If the MP3.com

¹⁰⁸ Id. at 1470-71. The court rejected the defendants' argument that its site was increasing hits to the plaintiffs' sites through referrals off its own site, noting that the defendants had not addressed how many hits to the plaintiffs' sites were diverted away as a consequence of the posting of articles to the Free Republic. The court also cited several cases rejecting the argument that a use is fair because it increases demand for the plaintiff's copyrighted work. Id. at 1471.

¹⁰⁹ Id. at 1472.

¹¹⁰ Id. at 1472-73.

¹¹¹ Los Angeles Times v. Free Republic, 56 U.S.P.Q. 2d 1862 (C.D. Cal. 2000).

¹¹² Complaint for Copyright Infringement, UMG Recordings, Inc. v. MP3.com, Inc., No. 00 Civ. 0472 (S.D.N.Y. Jan. 21, 2000).

¹¹³ Id. ¶ 4 & App. A.

server was able to recognize the CD, the user was then given access to the song tracks contained on the CD stored on an MP3.com server.¹¹⁴

In order to offer the My.MP3 service, MP3.com purchased and copied the tracks from several tens of thousands of commercial CDs onto its servers.¹¹⁵ When users accessed sound recordings through My.MP3, it was these reproductions made by MP3.com that were accessed, and not any copies made from the users' own CD.¹¹⁶ The plaintiffs sought a ruling that the copying of the commercial CDs onto the MP3.com servers constituted willful infringement of the copyright rights of the plaintiffs.

The case raised the very interesting issue of whether, assuming that users who are the owners of a lawful copy of a CD could lawfully upload a copy thereof to an MP3.com server for their own private use under Section 1008¹¹⁷ of the Audio Home Recording Act of 1992¹¹⁸ or under the fair use doctrine, it should be lawful for MP3.com to assist users in accomplishing that, and, if so, whether it should be permissible to do so by advance copying of tracks in anticipation of a user ordering or already owning a CD containing those tracks.

The court ruled that the copying by MP3.com of the commercial CDs made out a prima facie case of direct copyright infringement,¹¹⁹ and rejected the defendant's assertion that such copying was a fair use. The court ruled that the first fair use factor (purpose and character of the use) weighed against the defendant because the defendant's purpose for the use was commercial – although defendant was not charging users a fee for the service, “defendant seeks to attract a sufficiently large subscription base to draw advertising and otherwise make a profit.”¹²⁰ The court rejected the defendant's argument that the copying was transformative because it allowed users to “space shift” their CDs into another format in which they could enjoy their sound recordings without lugging around physical CDs, ruling that the argument was

¹¹⁴ Id.

¹¹⁵ UMG Recordings Inc. v. MP3.com Inc., 92 F. Supp. 2d 349, 350 (S.D.N.Y. 2000).

¹¹⁶ Id.

¹¹⁷ Section 1008 provides: “No action may be brought under this title alleging infringement of copyright based on the manufacture, importation, or distribution of a digital audio recording device, a digital audio recording medium, an analog recording device, or an analog recording medium, or based on the noncommercial use by a consumer of such a device or medium for making digital musical recordings or analog musical recordings.” 17 U.S.C. § 1008.

¹¹⁸ Pub. L. No. 102-563, 106 Stat. 4244 (1992).

¹¹⁹ “Thus, although defendant seeks to portray its service as the ‘functional equivalent’ of storing its subscribers’ CDs, in actuality defendant is re-playing for the subscribers converted versions of the recordings it copied, without authorization, from plaintiffs’ copyrighted CDs. On its face, this makes out a presumptive case of infringement under the Copyright Act of 1976” 92 F. Supp. 2d at 350.

¹²⁰ Id. at 351.

“simply another way of saying that the unauthorized copies are being retransmitted in another medium – an insufficient basis for any legitimate claim of transformation.”¹²¹

With respect to the second factor (nature of the copyrighted work), the court held that, because the copyrighted works at issue were creative musical works, this factor weighed against defendant.¹²² The third factor (amount and substantiality of the copyrighted work used) also weighed against the defendant because the defendant had copied, and the My.MP3 service replayed, the copyrighted works in their entirety.¹²³

Finally, with respect to the fourth factor (effect of the use upon the potential market for or value of the copyrighted work), the court noted that the defendant’s activities “on their face invade plaintiffs’ statutory right to license their copyrighted sound recordings to others for reproduction.”¹²⁴ The defendant argued that its activities enhanced the plaintiffs’ sales, since subscribers could not gain access to recordings through MP3.com unless had already purchased, or agreed to purchase, their own CD copies of those recordings. The court rejected this argument on the following rationale:

Any allegedly positive impact of defendant’s activities on plaintiffs’ prior market in no way frees defendant to usurp a further market that directly derives from reproduction of the plaintiffs’ copyrighted works. This would be so even if the copyright holder had not yet entered the new market in issue, for a copyright holder’s “exclusive” rights, derived from the Constitution and the Copyright Act, include the right, within broad limits, to curb the development of such a derivative market by refusing to license a copyrighted work or by doing so only on terms the copyright owner finds acceptable.¹²⁵

The court therefore ruled that the defendant was not entitled to a fair use defense as a matter of law, and entered partial summary judgment holding the defendant to have infringed the plaintiffs’ copyrights.¹²⁶ Subsequent to the court’s ruling of infringement, the defendant settled with all but one of the plaintiff record companies (Universal Music Group) by taking a license to reproduce the plaintiffs’ recordings on its servers and to stream them over the Internet to its subscribers, for which MP3.com reportedly paid \$20 million to each of the record

¹²¹ Id. Contrast this holding with the Ninth Circuit’s statement in RIAA v. Diamond Multimedia Sys., 180 F.3d 1072, 1079 (9th Cir. 1999), in which the Ninth Circuit found space shifting of a recording from a CD onto the “Rio” portable MP3 player device (through a process known as “ripping,” or re-encoding of music data encoded in CD format into the MP3 file format) to be “paradigmatic noncommercial personal use entirely consistent with the purposes of the [Audio Home Recording Act].”

¹²² UMG, 92 F. Supp. 2d at 351-52.

¹²³ Id. at 352.

¹²⁴ Id.

¹²⁵ Id. (citations omitted).

¹²⁶ Id. at 353.

companies and agreed to pay a few pennies each time a user placed a CD in his or her locker, plus a smaller amount each time a track was played.¹²⁷

Universal Music Group pursued a claim of statutory damages against MP3.com. The court concluded that MP3.com's infringement was willful, and awarded statutory damages of \$25,000 per CD illegally copied by MP3.com.¹²⁸ Even based on the defendant's assertion that there were no more than 4,700 CDs for which the plaintiffs qualified for statutory damages (an issue that was to have been the subject of a separate trial), the statutory damages award would have come to \$118,000,000.¹²⁹ On the eve of trial, the defendant settled with Universal Music Group by agreeing to pay the plaintiff \$53.4 million and to take a license to Universal's entire music catalog in exchange for unspecified royalty payments.¹³⁰

MP3.com's legal troubles did not end with the settlements with the RIAA plaintiffs. On Aug. 8, 2001, a group of over 50 music publishers and songwriters filed suit against MP3.com on claims of copyright infringement very similar to those asserted by the RIAA plaintiffs. The plaintiffs sought to hold MP3.com liable for the copies of their works made in connection with the My.MP3.com service, as well as for the subsequent "viral distribution" of copies of their works allegedly done through services such as Napster, Gnutella, Aimster, and Music City by MP3.com users after they download digital copies through MP3.com.¹³¹ Numerous other suits were brought against MP3.com as well. For example, in Sept. of 2001, Isaac, Taylor & Zachary Hanson also sued MP3.com for copying of their copyrighted songs on My.MP3.com.¹³²

Numerous opinions have been issued as a result of these lawsuits, holding MP3.com liable for willful copyright infringement and ruling it collaterally estopped from denying that it

¹²⁷ See Jon Healey, "MP3.com Settles with BMG, Warner," *San Jose Mercury News* (June 10, 2000), at 1A; Chris O'Brien, "MP3 Sets Final Pact: Universal Music Group Will Get \$53.4 Million," *San Jose Mercury News* (Nov. 15, 2000) at 1C, 14C.

¹²⁸ *UMG Recordings Inc. v. MP3.com, Inc.*, 56 U.S.P.Q.2d 1376, 1379, 1381 (S.D.N.Y. 2000). The court rejected the plaintiffs' argument that a statutory damages award should be made for each song copied, rather than each CD. The court cited 17 U.S.C. § 504(c)(1), which provides that a statutory damages award may be recovered in a specified range "with respect to any one work," and further provides that "all parts of a compilation or derivative work constitute one work." *UMG Recordings Inc. v. MP3.com Inc.*, 109 F. Supp. 2d 223, 224-25 (S.D.N.Y. 2000).

¹²⁹ 56 U.S.P.Q.2d at 1381.

¹³⁰ O'Brien, *supra* note 127, at 1C.

¹³¹ "Music Publishers, Songwriters Sue MP3.com for 'Viral Distribution' of Copyrighted Works," *BNA's Electronic Commerce & Law Report* (Aug. 29, 2001) at 933. In late August of 2001, MP3.com was acquired by media company Vivendi Universal.

¹³² Steven Bonisteel, "Hanson Sues Music Locker Service Over Copyright" (Sept. 26, 2001), available as of Jan. 6, 2002 at www.newsbytes.com/news/01/170530.html.

willfully infringed the plaintiffs' various copyrighted works when it created the "server copies" of thousands of CDs in late 1999 and early 2000.¹³³

(i) The CoStar Case

In CoStar Group Inc. v. LoopNet, Inc.,¹³⁴ the plaintiff CoStar maintained a copyrighted commercial real estate database that included photographs. The defendant LoopNet offered a service through which a user, usually a real estate broker, could post a listing of commercial real estate available for lease. The user would access, fill out, and submit a form for the property available. To include a photograph of the property, the user was required to fill out another form. The photograph would initially be uploaded into a separate folder on LoopNet's system, where it would first be reviewed by a LoopNet employee to determine that it was in fact a photograph of commercial property and that there was no obvious indication the photograph was submitted in violation of LoopNet's terms and conditions. If the photograph met LoopNet's criteria, the employee would accept it and post it along with the property listing. CoStar claimed that over 300 of its copyrighted photographs had been posted on LoopNet's site, and sued LoopNet for both direct and contributory copyright liability.¹³⁵

CoStar argued that LoopNet should be directly liable for copyright infringement because, acting through its employees' review and subsequent posting of the photographs, LoopNet was directly copying and distributing the photographs, citing the Frena case discussed above in Section II.A.4(d). The district court rejected this argument, noting that the Fourth Circuit in the ALS Scan case had concluded that the legislative history of the DMCA indicated Congress' intent to overrule the Frena case and to follow the Netcom case, under which an OSP's liability for postings by its users must be judged under the contributory infringement doctrine.¹³⁶

The Fourth Circuit affirmed this ruling on appeal.¹³⁷ Citing its own decision in the ALS Scan case, the Fourth Circuit noted that it had already held that the copyright statute implies a requirement of volition or causation, as evidenced by specific conduct by the purported infringer, for direct liability.¹³⁸ Mere ownership of an electronic facility by an OSP that responds automatically to users' input is not sufficient volition for direct liability. "There are thousands of owners, contractors, servers, and users involved in the Internet whose role involves the storage and transmission of data in the establishment and maintenance of an Internet facility. Yet their

¹³³ See, e.g., Country Road Music, Inc. v. MP3.com, Inc., 279 F.Supp.2d 325 (S.D.N.Y. 2003); Zomba Enters., Inc. v. MP3.com, Inc., No. 00 Civ. 6833 (S.D.N.Y. Jun. 8, 2001); Teevee Toons, Inc. v. MP3.com, Inc., 134 F. Supp. 2d 546 (S.D.N.Y. 2001); UMG Recordings, Inc. v. MP3.com, Inc., No. 00 Civ. 472, 200 WL 1262568 (S.D.N.Y. 2000).

¹³⁴ 164 F. Supp. 2d 688 (D. Md. 2001).

¹³⁵ Id. at 691-92.

¹³⁶ Id. at 695-96.

¹³⁷ CoStar v. LoopNet, 373 F.3d 544 (4th Cir. 2004).

¹³⁸ Id. at 549.

conduct is not truly ‘copying’ as understood by the Act; rather, they are conduits from or to would-be copiers and have no interest in the copy itself.”¹³⁹

The court also inferred a requirement of volition from the statute’s concept of “copying,” which requires the making of “fixed” copies. For the reasons discussed in Section II.A.2 above, the court concluded that transient copies made by an OSP acting merely as a conduit to transmit information at the instigation of others does not create sufficiently fixed copies to make it a direct infringer of copyright.¹⁴⁰ Accordingly, the court concluded, “[a]greeing with the analysis in Netcom, we hold that the automatic copying, storage and transmission of copyrighted materials, when instigated by others, does not render an ISP strictly liable for copyright infringement under §§ 501 and 106 of the Copyright Act.”¹⁴¹ The court also affirmed the district court’s ruling that the quick review of photographs performed by LoopNet’s employees before allowing them to be posted on the site did not amount to “copying,” nor did it add volition to LoopNet’s involvement in storing the copy.¹⁴²

(j) The Ellison Case

The case of Ellison v. Robertson,¹⁴³ discussed in detail in Section III.C.6(b)(1)(i) below, refused to hold an OSP liable for direct infringement based on infringing materials posted on its service by users without its knowledge on Usenet servers hosted by AOL (infringing copies of fictional works).

(k) Perfect 10 v. Cybernet Ventures

In Perfect 10, Inc. v. Cybernet Ventures, Inc.,¹⁴⁴ the court refused to hold the defendant Cybernet, an “age verification service” that enrolled subscribers, after verifying their age as an adult, to a service that would enable them to gain access for a monthly fee to a large number of member sites displaying pornographic pictures, liable as a direct copyright infringer based on the unauthorized presence of the plaintiffs’ copyrighted photographs on several of the member sites. The court discussed the Netcom, MAPHIA, and Hardenburgh cases (the Hardenburgh case is discussed in Section II.C below), then concluded as follows:

The principle distilled from these cases is a requirement that defendants must actively engage in one of the activities recognized in the Copyright Act. Based on the evidence before the Court it appears that Cybernet does not use its hardware to either store the infringing images or move them from one location to another for display. This technical

¹³⁹ Id. at 551.

¹⁴⁰ Id.

¹⁴¹ Id. at 555.

¹⁴² Id. at 556.

¹⁴³ 189 F. Supp. 2d 1051 (C.D. Cal. 2002), aff’d in part and rev’d in part, 357 F.3d 1072 (9th Cir. 2004) (district court’s ruling of no direct infringement not challenged on appeal).

¹⁴⁴ 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

separation between its facilities and those of its webmasters prevents Cybernet from engaging in reproduction or distribution, and makes it doubtful that Cybernet publicly displays the works. Further, there is currently no evidence that Cybernet has prepared works based upon Perfect 10's copyrighted material. The Court therefore concludes that there is little likelihood that Perfect 10 will succeed on its direct infringement theory.¹⁴⁵

(I) Field v. Google

In Field v. Google,¹⁴⁶ discussed in greater detail in Section III.B.4(a) below, the court ruled that Google should not be liable as a direct infringer for serving up through its search engine, in response to user search queries, copies of the plaintiff's copyrighted materials that had been cached by Google's automated crawler, the Googlebot. Citing the Netcom and CoStar cases, the court noted that a plaintiff must "show volitional conduct on the part of the defendant in order to support a finding of direct copyright infringement."¹⁴⁷ For some unknown reason, the plaintiff did not allege that Google committed infringement when its Googlebot made the initial copies of the plaintiff's Web pages on which his copyrighted materials had been placed and stored those copies in the Google cache, nor did the plaintiff assert claims for contributory or vicarious liability. Instead, the plaintiff alleged that Google directly infringed his copyrights when a Google user clicked on a link on a Google search results page to the Web pages containing his copyrighted materials and downloaded a cached copy of those pages from Google's computers.¹⁴⁸

The court rejected this argument:

According to Field, Google itself is creating and distributing copies of his works. But when a user requests a Web page contained in the Google cache by clicking on a "Cached" link, it is the user, not Google, who creates and downloads a copy of the cached Web page. Google is passive in this process. Google's computers respond automatically to the user's request. Without the user's request, the copy would not be created and sent to the user, and the alleged infringement at issue in this case would not occur. The automated, non-volitional conduct by Google in response to a user's request does not constitute direct infringement under the Copyright Act.¹⁴⁹

¹⁴⁵ Id. at 1168-69.

¹⁴⁶ 412 F. Supp. 2d 1106 (D. Nev. 2006).

¹⁴⁷ Id. at 1115.

¹⁴⁸ Id.

¹⁴⁹ Id.

(m) Parker v. Google

In Parker v. Google,¹⁵⁰ pro se plaintiff Gordon Parker was the owner of copyright in an e-book titled “29 Reasons Not To Be A Nice Guy.” He posted Reason # 6 on USENET. Parker asserted that Google’s automatic archiving of this USENET posting constituted a direct infringement of his copyright. He also claimed that when Google produced a list of hyperlinks in response to a user’s query and excerpted his web site in that list, Google again directly infringed his copyrighted work.¹⁵¹

The district court rejected these claims. Citing the Costar and Netcom cases, the district court held that “when an ISP automatically and temporarily stores data without human intervention so that the system can operate and transmit data to its users, the necessary element of volition is missing. The automatic activity of Google’s search engine is analogous. It is clear that Google’s automatic archiving of USENET postings and excerpting of websites in its results to users’ search queries do not include the necessary volitional element to constitute direct copyright infringement.”¹⁵²

On appeal, the Third Circuit affirmed in an unpublished decision.¹⁵³ The court noted that, “to state a direct copyright infringement claim, a plaintiff must allege volitional conduct on the part of the defendant,” and Parker’s allegations failed to allege any volitional conduct on the part of Google.¹⁵⁴

(n) The Cablevision Case

In Twentieth Century Fox Film Corp. v. Cablevision Sys.,¹⁵⁵ the district court ruled that Cablevision was liable for direct copyright infringement based on the offering of a network digital video recording system known as the “Remote-Storage DVR System” (RS-DVR), which permitted customers to record cable programs on central servers at Cablevision’s facilities and play the programs back for viewing at home. The technology underlying the RS-DVR worked as follows. Cablevision took the linear programming signal feed received at its head end and reconfigured it by splitting the feed into a second stream, which was then reformatted through a process known as “clamping” to convert the bitrate of the stream into one that was more efficient. In the process of clamping, portions of programming were placed into buffer memory. The stream was then converted into a number of single program transport streams, one channel per stream. The converted streams were then fed into a special set of “Arroyo” servers, which at any given

¹⁵⁰ 422 F. Supp. 2d 492 (E.D. Pa. 2006), aff’d, 2007 U.S. App. LEXIS 16370 (3d Cir. July 10, 2007).

¹⁵¹ Id. at 496.

¹⁵² Id. at 497.

¹⁵³ Parker v. Google, 2007 U.S. App. LEXIS 16370 (3d Cir. July 10, 2007).

¹⁵⁴ Id. at *6, 8.

¹⁵⁵ 478 F. Supp. 2d 607 (S.D.N.Y. 2007), rev’d, 536 F.3d 121 (2d Cir. 2008), cert. denied sub nom. CNN, Inc. v. CSC Holdings, Inc., 557 U.S. 946 (2009).

moment in time, stored in a buffer three frames of video from each of the linear channels carried by Cablevision, so that if a customer requested that a particular program be recorded, the appropriate packets could be retrieved from the buffer memory and copied to the customer's designated hard drive storage space on the Arroyo server.¹⁵⁶

The RS-DVR service allowed customers to request that a program be recorded in one of two ways. The customer could navigate an on-screen program guide and select a future program to record, or while watching a program, the customer could press a "record" button on a remote control. In response, the Arroyo server would receive a list of recording requests, find the packets for the particular programs requested for recording, then make a copy of the relevant program for each customer that requested it be recorded. A separate copy would be stored in each customer's designated hard drive storage space on the Arroyo server. If no customer requested that a particular program be recorded, no copy of that program was made on the hard drives of the Arroyo server. When the customer selected a recorded program for playback, the Arroyo server would locate the copy of the desired program stored on the customer's designated hard drive storage space, then cause the program to be streamed out. The stream containing the program would be transmitted to every home in the node where the requesting customer was located, but only the requesting set-top box would be provided the key for decrypting the stream for viewing.¹⁵⁷

The plaintiffs alleged direct copyright infringement based on Cablevision's creation of the copies on the hard drives of the Arroyo servers and of the buffer copies. Although Cablevision did not deny that these copies were being made, it argued that it was entirely passive in the process and the copies were being made by its customers. It also argued, based on the Sony case, that it could not be liable for copyright infringement for merely providing customers with the machinery to make the copies.¹⁵⁸

The court rejected these arguments, ruling that the RS-DVR was not merely a device, but rather a service, and that, by providing the service, it was Cablevision doing the copying. In particular, the court found the relationship between Cablevision and RS-DVR customers to be significantly different from the relationship between Sony and VCR users. Unlike a VCR, the RS-DVR did not have a stand-alone quality. Cablevision retained ownership of the RS-DVR set-top box, and the RS-DVR required a continuing relationship between Cablevision and its customers. Cablevision not only supplied the set-top box for the customer's home, but also decided which programming channels to make available for recording, and housed, operated, and maintained the rest of the equipment that made the RS-DVR's recording process possible. Cablevision also determined how much memory to allot to each customer and reserved storage capacity for each

¹⁵⁶ Id. at 613-14.

¹⁵⁷ Id. at 614-16.

¹⁵⁸ Id. at 617-18.

customer on a hard drive at its facility. Customers were offered the option of acquiring additional capacity for a fee.¹⁵⁹

In sum, the court concluded that the RS-DVR was more akin to a video-on-demand (VOD) service than to a VCR or other time-shifting device. The court noted that the RS-DVR service was in fact based on a modified VOD platform. With both systems, Cablevision decided what content to make available to customers for on-demand viewing. As in VOD, the number of available pathways for programming delivery was limited; if there were none available, the customer would get an error message or busy signal. Thus, in its architecture and delivery method, the court concluded that the RS-DVR bore a striking resemblance to a VOD service – a service that Cablevision provided pursuant to licenses negotiated with programming owners.¹⁶⁰ Accordingly, the court ruled that a reasonable fact finder could conclude only that the copying at issue was being done not by the customers, but by Cablevision itself.¹⁶¹

With respect to the buffer copies, Cablevision argued that the buffer copies were not sufficiently fixed to be cognizable as “copies” under copyright law. The court rejected this argument, noting that the buffer copies were sufficiently permanent to make the Arroyo hard disk copies from, and were therefore capable of being reproduced, as required by the definition of “fixation.” The court also cited the numerous court decisions, and the Copyright Office’s August 2001 report on the DMCA, concluding that RAM copies are “copies” for purposes of the copyright act. Accordingly, the court concluded that summary judgment of direct infringement was warranted with respect to both the Arroyo server copies and the buffer copies.¹⁶²

Finally, the court ruled, based on similar logic, that Cablevision was engaged in infringing transmissions and public performances to its customers.¹⁶³ The court noted that, “where the relationship between the party sending a transmission and party receiving it is commercial, as would be the relationship between Cablevision and potential RS-DVR customers, courts have determined that the transmission is one made ‘to the public.’”¹⁶⁴

On appeal, the Second Circuit reversed in The Cartoon Network LP v. CSC Holdings, Inc.¹⁶⁵ The Second Circuit’s rulings with respect to the issue of buffer copies are discussed in Section II.A.2 above. With respect to the copies created on the hard drives of the Arroyo servers, the court noted that Netcom and its progeny direct attention to the volitional conduct that causes the copy to be made. In the case of an ordinary VCR, the court noted that it seemed clear that the operator of the VCR – the person actually pressing the button to make the recording,

¹⁵⁹ Id. at 618-19.

¹⁶⁰ Id. at 619.

¹⁶¹ Id. at 621.

¹⁶² Id. at 621-22.

¹⁶³ Id. at 622-23.

¹⁶⁴ Id. at 623.

¹⁶⁵ 536 F.3d 121 (2d Cir. 2008), cert. denied sub nom. CNN, Inc. v. CSC Holdings, Inc., 557 U.S. 946 (2009).

supplies the necessary element of volition, not the manufacturer of the device. The court concluded that the RS-DVR customer was not sufficiently distinguishable from a VCR user to impose liability as a direct infringer on a different party for copies that were made automatically upon that customer's command. The court distinguished cases holding liable a copy shop making course packs for college professors, finding a significant difference between making a request to a human employee, who then voluntarily operates the copying system to make the copy, and issuing a command directly to a system, which automatically obeys commands and engages in no volitional conduct.¹⁶⁶ "Here, by selling access to a system that automatically produces copies on command, Cablevision more closely resembles a store proprietor who charges customers to use a photocopier on his premises, and it seems incorrect to say, without more, that such a proprietary 'makes' any copies when his machines are actually operated by his customers."¹⁶⁷

Nor was Cablevision's discretion in selecting the programming that it would make available for recording sufficiently proximate to the copying to displace the customer as the person who "made" the copies. Cablevision's control was limited to the channels of programming available to a customer and not to the programs themselves. Cablevision had no control over what programs were made available on individual channels or when those programs would air, if at all. In that respect, Cablevision possessed far less control over recordable content than it did in the VOD context, where it actively selected and made available beforehand the individual programs available for viewing. Thus, Cablevision could not have direct liability for the acts of its customers, and any liability on its part would have to be based on contributory liability. The district court's noted "continuing relationship" with its RS-DVR customers, its control over recordable content, and the instrumentality of copying would be relevant to contributory liability, but not direct liability.¹⁶⁸

With respect to the issue of direct liability, the Second Circuit concluded: "We need not decide today whether one's contribution to the creation of an infringing copy may be so great that it warrants holding that party directly liable for the infringement, even though another party has actually made the copy. We conclude only that on the facts of this case, copies produced by the RS-DVR system are 'made' by the RS-DVR customer, and Cablevision's contribution to this reproduction by providing the system does not warrant the imposition of direct liability."¹⁶⁹

The Second Circuit's rulings with respect whether Cablevision was engaged in unauthorized public performances through the playback of the RS-DVR copies are discussed in Section II.B.5 below.

¹⁶⁶ Id. at 131.

¹⁶⁷ Id. at 132.

¹⁶⁸ Id. at 132-33.

¹⁶⁹ Id. at 133.

(o) Arista Records v. Usenet.com

In Arista Records LLC. v. Usenet.com, Inc.,¹⁷⁰ the defendants operated a Napster-like Usenet service that advertised to and targeted users who wanted to download music files. Unlike peer-to-peer filing sharing networks, the files were stored on “spool” news servers operated by the defendants. The defendants created designated servers for newsgroups containing music binary files to increase their retention time over other types of Usenet files.¹⁷¹

The plaintiffs contended that the defendants directly infringed their copyrights by engaging in unauthorized distribution of copies of their musical works to subscribers who requested them for download. The court, relying on the Netcom and Cablevision cases, ruled that a finding of direct infringement of the distribution right required a showing that the defendants engaged in some volitional conduct sufficient to show that they actively participated in distribution of copies of the plaintiffs’ copyrighted sound recordings. The court found sufficient volitional conduct from the following facts. The defendants were well aware that digital music files were among the most popular files on their service, and took active measures to create spool servers dedicated to MP3 files and to increase the retention times of newsgroups containing digital music files. They took additional active steps, including both automated filtering and human review, to remove access to certain categories of content (such as pornography), while at the same time actively targeting young people familiar with other file-sharing programs to try their services as a supposedly safe alternative to peer-to-peer music file sharing programs that were getting shut down for infringement. From these facts, the court ruled that the defendants’ service was not merely a passive conduit that facilitated the exchange of content between users who uploaded infringing content and users who downloaded such content, but rather the defendants had so actively engaged in the distribution process so as to satisfy the volitional conduct requirement. Accordingly, the court granted the plaintiffs’ motion for summary judgment on their claim for direct infringement of the distribution right.¹⁷²

(p) Quantum Systems v. Sprint Nextel

In Quantum Sys. Integrators, Inc. v. Sprint Nextel Corp.,¹⁷³ Quantum sued Sprint for copyright infringement based on the automated loading of Quantum’s software into the RAM of 13 Sprint computers from unauthorized copies on the hard disk when those computers were turned on or rebooted. The jury found liability and Sprint argued on appeal that the district court erred in denying its JMOL motion and sustaining the jury’s finding of infringement because there was no evidence that Sprint engaged in volitional copying, since the RAM copies were

¹⁷⁰ 633 F. Supp. 2d 124 (S.D.N.Y. 2009).

¹⁷¹ Id. at 130-31.

¹⁷² Id. at 132, 146-49. As a sanction for litigation misconduct, including spoliation of evidence and sending key employees out of the country on paid vacations so they could not be deposed, the court precluded the defendants from asserting an affirmative defense of protection under the DMCA’s safe harbor provisions. Id. at 137-42.

¹⁷³ 2009 U.S. App. LEXIS 14766 (4th Cir. July 7, 2009).

automatically generated when the computers containing unauthorized, but unutilized, copies of the software on the hard disk were turned on. The court rejected this argument, distinguishing its Costar decision, which involved an ISP that merely provided electronic infrastructure for copying, storage, and transmission of material at the behest of its users. By contrast, in the instant case the copying was instigated by the volitional acts of Sprint's own employees who loaded the original copies of the software onto Sprint computers and then rebooted the computers, thereby causing the RAM copies.¹⁷⁴

(q) **Arista Records v. Myxer**

In Arista Records LLC v. Myxer Inc.,¹⁷⁵ the defendant Myxer operated a website that enabled registered users to upload recorded music to the site and then, through the use of Myxer's software, to transcode the music into a format to create and download ringtones. Users could make ringtones they had created available for download to other users. In addition to uploading and downloading ringtones, Myxer users could play portions of any of the sound recordings on Myxer's site. Users could also select a sound recording on Myxer's site and share it on certain third party websites such as Facebook. Finally, users could select a sound recording on Myxer's site, often a full-length recording, and "Customize It" (using editing tools provided by Myxer) by selecting a desired start and stop point for a ringtone. UMG Records, a competitor in the ringtone market, contended that, by storing copies of UMG's sound recordings on its servers, allowing users to download copies of its sound recordings to users' cell phones, and allowing users to preview its sound recordings on either the Myxer site or on users' cell phones, Myxer was a direct infringer of UMG's reproduction, distribution and digital public performance rights, as well as a secondary infringer under theories of contributory and vicarious liability.¹⁷⁶

UMG moved for summary judgment on its direct infringement claim. Myxer opposed such motion based on the volitional requirement for direct liability under Netcom and other cases, arguing that the user, not Myxer, engaged in the acts of direct copying, distribution, and public performance (if any). The court found that the undisputed facts in the case established a prima facie case that Myxer had directly infringed at least one of UMG's exclusive rights.¹⁷⁷ The court noted that it was "well-established that copyright infringement is a strict liability tort: there is no need to prove the defendant's mental state to establish copyright infringement."¹⁷⁸ Given that fact, and the fact that the Ninth Circuit had never expressly adopted a volitional conduct requirement as an element of direct liability, the court concluded that it was not inclined to adopt such a requirement absent clear instruction from the Ninth Circuit.¹⁷⁹ (Note, however, that the Ninth Circuit subsequently did expressly adopt a volitional conduct requirement as an

¹⁷⁴ Id. at *1-3 & *15-18.

¹⁷⁵ 2011 U.S. Dist. LEXIS 109668 (C.D. Cal. Apr. 1, 2011).

¹⁷⁶ Id. at *2, 15-18.

¹⁷⁷ Id. at *37-39.

¹⁷⁸ Id. at *45.

¹⁷⁹ Id. at *46-49.

element of direct liability in the Fox Broadcasting v. Dish Network case discussed in Section II.A.4(u) below.) Nevertheless, the court denied UMG's motion for summary judgment because of genuine issues of material fact pertaining to Myxer's assertion of the safe harbor of Section 512(c), as discussed in Section III.C.6(b)(1)(iii).r below.¹⁸⁰

The court also denied UMG's motion for summary judgment with respect to its claims of contributory and vicarious liability. With respect to contributory liability, the court noted that there were substantial noninfringing uses of the Myxer site, because many of the ringtones and recordings available were directly authorized by their copyright holder or users had certified that they controlled the rights. Nevertheless, the court found summary judgment to be inappropriate because contributory infringement requires a showing of direct copyright infringement, which had not yet been definitively established. With respect to vicarious liability, the court noted that, to the extent Myxer used the Audible Magic filtering technology to keep infringing material from being uploaded onto its site, as well as other means to stop or limit the alleged copyright infringement, there were genuine issues of material fact as to whether Myxer sufficiently exercised a right to stop or limit the alleged copyright infringement. And, as in the case of contributory infringement, it remained unclear whether there was an underlying claim of direct infringement.¹⁸¹

(r) Disney Enterprises v. Hotfile

In Disney Enterprises, Inc. v. Hotfile Corp.,¹⁸² the defendant operated the web site www.hotfile.com, at which users could upload electronic files to Hotfile's servers. Upon upload, the user received a unique link to the file. The Hotfile servers would then automatically make five additional copies of the uploaded files and assign each copy a unique link. Each link acted as a locator, allowing anyone with the link to click it or plug it into a web browser in order to download the file. Third party sites, not Hotfile, catalogued, allowed searching of, and/or spread the links that allowed persons to download the files.¹⁸³

Hotfile made a profit in two ways. First, although anyone could use a link to download a file, Hotfile charged members a fee that enabled them to download files much faster than non-members. Second, Hotfile sold "hotlinks" that allowed third party sites to post a link that, when clicked, automatically began to download the file, without ever directing the person clicking the link to hotfile.com. To increase its number of members, Hotfile paid users to upload the most popular content to its servers and asked that the users promote their links. Hotfile's affiliate program, for example, paid those uploading files cash when the file was downloaded 1000 times. The complaint alleged that, as a result of their popularity, copyright-infringing files constituted the bulk of files downloaded through Hotfile, Hotfile's business encouraged persons to upload

¹⁸⁰ Id. at *3.

¹⁸¹ Id. at *137-141. The court also concluded that as a matter of law, Myxer's use of UMG's works did not qualify as fair use. See id. at *109-135.

¹⁸² 798 F. Supp. 2d 1303 (S.D. Fla. 2011).

¹⁸³ Id. at 1306.

material with copyright protection, and Hotfile understood the consequences of its business model.¹⁸⁴

The defendants filed a motion to dismiss the plaintiff's claims for direct and secondary liability for copyright infringement. The court granted the motion as to direct infringement, invoking the requirement of Netcom that there must be some volitional act on the part of the defendant in making the copies in order to establish direct liability. Here the hotfile.com web site merely allowed users to upload and download copyrighted material without volitional conduct on the part of the defendants.¹⁸⁵ The court found unpersuasive two cases relied on by the plaintiffs, the Mp3Tunes¹⁸⁶ and Usenet.com¹⁸⁷ cases, to support their argument that the defendants, by creating a plan that induced infringement, were liable for direct infringement. Although the court noted that the two cases supported the plaintiffs' argument, the court stated that it believed the cases were not correctly decided. The court also rejected the plaintiffs' attempt to distinguish Netcom on the ground that it applied only where a defendant violated a copyright holder's right to reproduce – but not to distribute. The court noted that the Netcom court stated it considered the copyright holder's right to distribute in its analysis. The court also rejected the plaintiffs' argument that they had alleged a volitional act in the form of Hotfile's making of additional copies once the copyrighted material was uploaded to its server, because courts had repeatedly held that the automatic conduct of software, unaided by human intervention, is not volitional.¹⁸⁸

The court found, however, that the plaintiffs had adequately pled claims for inducement, contributory, and vicarious liability. Inducement and contributory infringement were adequately pled by allegations that hotfile.com was a web site that Hotfile used to promote copyright infringement and that Hotfile took affirmative steps to foster the infringement by creating a structured business model that encouraged users to commit copyright infringement. Vicarious liability was adequately pled by allegations that Hotfile had complete control over the servers that users employed to infringe, had the technology necessary to stop the infringement, refused to stop the massive infringement, and actually encouraged the infringement because the infringement increased its profits.¹⁸⁹

¹⁸⁴ Id. at 1306-07.

¹⁸⁵ Id. at 1307-08.

¹⁸⁶ Capitol Records, Inc. v. Mp3Tunes, LLC, 2009 U.S. Dist. LEXIS 96521 (S.D.N.Y. Oct. 16, 2009), which held, without much analysis, that a company's knowledge of massive infringement plausibly alleged volitional conduct.

¹⁸⁷ Arista Records LLC v. Usenet.com, Inc. 633 F. Supp. 2d 124 (S.D.N.Y. 2009), which held that a company, having a policy encouraging infringement plus the ability to stop that infringement, was liable for direct copyright infringement.

¹⁸⁸ Hotfile, 798 F. Supp. 2d at 1307-09.

¹⁸⁹ Id. at 1301.

The court's subsequent rulings upon various motions for summary judgment with respect to the DMCA safe harbors and secondary liability are discussed in Sections III.C.3(s), III.C.4(f) and III.C.6(b)(1)(iii).y below.

In Dec. 2013, the MPAA announced a settlement under which the district court had awarded damages of \$80 million to the plaintiffs and ordered Hotfile to either shut down its operations or use digital fingerprinting technology to prevent copyright infringement by its users.¹⁹⁰

(s) Perfect 10 v. Megaupload

In Perfect 10, Inc. v. Megaupload Limited,¹⁹¹ the defendant operated a file storage service through the "Megaupload" web site (among others), which allowed users to upload files. After upload, the web site created a unique URL to the file, and anyone with the URL could then download the file from Megaupload's servers. Both Megaupload and its users disseminated URLs for various files throughout the Internet. In order to view, copy, or download files from the web sites without a waiting period, users were required to pay a membership fee. The plaintiff sued the defendants for direct and secondary copyright infringement because thousands of its copyrighted photographs were uploaded to Megaupload and available for downloading. Those photos contained copyright notices and were labeled "Perfect 10" or "Perfect-10." The complaint alleged that Megaupload depended on, and provided substantial payouts to, affiliate web sites who catalogued the URLs providing access to a mass of pirated content on Megaupload's servers, and that Megaupload encouraged its users to upload materials through a rewards program. The defendant moved to dismiss the direct and secondary liability claims.¹⁹²

With respect to the direct infringement claim, the court noted that under Netcom, an important element of direct infringement is volitional conduct, and the element of volitional conduct applies to all exclusive rights under the copyright act.¹⁹³ Drawing all reasonable inferences in the plaintiff's favor, the court found that the plaintiff had adequately pled a claim for direct infringement:

Megaupload serves as more than a passive conduit, and more than a mere "file storage" company: it has created distinct websites, presumably in an effort to streamline users' access to different types of media (e.g., megaporn.com, megavideo.com); it encourages and, in some cases pays, its users to upload vast amounts of popular media through its Rewards Programs; it disseminates URLs for various files throughout the internet; it provides payouts to affiliate websites who maintain a catalogue of all available files; and,

¹⁹⁰ "Hotfile To Pay \$80M to MPAA, Studios In Copyright Suit," *Law360* (Dec. 3, 2013), available as of Dec. 7, 2013 at http://www.law360.com/ip/articles/493076?nl_pk=be5fde4e-8dc1-4d81-b621-f0352bcdff74&utm_source=newsletter&utm_medium=email&utm_campaign=ip.

¹⁹¹ 2011 U.S. Dist. LEXIS 81931 (S.D. Cal. July 27, 2011).

¹⁹² *Id.* at *3-5.

¹⁹³ *Id.* at *10.

last, at a minimum, it is plausibly aware of the ongoing, rampant infringement taking place on its websites. Taken together, Perfect 10 has adequately alleged Megaupload has engaged in volitional conduct sufficient to hold it liable for direct infringement.¹⁹⁴

The court also concluded that claims of contributory infringement were adequately pled. Knowledge of infringement had been adequately pled because, in addition to takedown notices (which the court noted doubt as to whether takedown notices automatically imply knowledge), many of the allegations giving rise to direct infringement also gave rise to knowledge. The plaintiff had also adequately pled a material contribution to infringement in that Megaupload encouraged, and in some cases, paid its users to upload vast amounts of popular media through its rewards programs, disseminated URLs that provided access to such media, and provided payouts to affiliates who catalogued the URLs for all available media.¹⁹⁵

The court concluded, however, that the plaintiff had not adequately pled claims of vicarious liability, because it did not allege facts suggesting that Megaupload had the right and ability to supervise infringing conduct of its third party users. Accordingly, the court dismissed the claim for vicarious liability without prejudice.¹⁹⁶

(t) Wolk v. Kodak Imaging Network

This case, which refused to find direct liability on the part of Kodak Imaging Network for lack of volitional conduct, is discussed in Section III.C.6(b)(1)(iii).q below.

(u) Fox Broadcasting v. Dish Network

The First Preliminary Injunction Ruling

Fox sought a preliminary injunction against Dish Network, which had a contract with Fox granting it the right to retransmit Fox broadcast material to its subscribers, for offering a high definition digital video recorder called the “Hopper” and two associated services called “PrimeTime Anytime” (PTAT) and “AutoHop.” Because the Hopper was designed to service multiple televisions, it had three tuners and a two-terabyte hard drive, which allowed Hopper users to watch or record on three different television stations at once. The Hopper had the additional unique capability of streaming all four of the major television networks on a single satellite transponder, which allowed a user to watch or record all four network broadcasts while leaving the other two tuners available for recording non-network programs or watching them on other television sets equipped with additional set top boxes. The PTAT feature allowed subscribers to set a single timer on the Hopper to record all primetime programming on any of the four major broadcast networks each night of the week. Dish determined the start and end time of the primetime block each night. In order to use PTAT, the user had to specifically enable

¹⁹⁴ Id. at *11-12 (citations to the complaint omitted).

¹⁹⁵ Id. at *16-17.

¹⁹⁶ Id. at *19.

it from the main menu. Once enabled, a screen appeared allowing the user to choose to disable recordings of certain networks on certain days of the week. If the user did not select otherwise, the default settings caused the Hopper to record the entire primetime window on all four of the major networks every day of the week. A user could begin watching the recorded programs immediately after PTAT started recording, and could cancel a particular PTAT recording on a given day up until 20 minutes before primetime programming began. All PTAT recordings were stored locally on the Hopper in users' homes. Unless the user selected otherwise, PTAT recordings were automatically deleted after eight days. The Hopper also worked with the "Sling Adapter," which allowed subscribers to view Hopper content on their computers and mobile devices via the Internet.¹⁹⁷

AutoHop was a feature that allowed users to skip commercials in PTAT recordings with the click of their remote control. If AutoHop was available for a particular PTAT program, the user was given the option to enable it for that show. If the user enabled AutoHop, the Hopper would automatically skip commercial breaks during that program. Markers inserted into the PTAT recordings to mark the beginning and end of the commercials were checked manually by technicians who viewed a separate quality assurance ("QA") copy of the recording made by Dish and stored on its servers. The technician would view the QA recording, fast-forwarding through the program itself to the commercial breaks, to ensure that the markings were accurate and no portion of the program was cut off. If the QA copies revealed an error in the marking process, technicians could correct the error on a later broadcast to ensure that AutoHop functioned properly for users who enabled it. If there was not enough time to correct a marking error before the last broadcast ended, then AutoHop would not be available for that particular show.¹⁹⁸

Fox sought a preliminary injunction against the PTAT and AutoHop functions on grounds of copyright infringement. The court turned first to whether Fox could have secondary liability for any infringing acts of its subscribers. Applying the Supreme Court's Sony case, the court noted that nothing suggested Hopper users were using the PTAT copies for anything other than time-shifting in their homes or on mobile devices, an activity determined to be a fair use in Sony. Because there was therefore no direct infringement on the part of PTAT users, Dish could not have secondary copyright liability.¹⁹⁹

The court then turned to whether Dish could have liability for direct copyright infringement for the making of the PTAT copies or the QA copies of Fox's programming. Citing the Netcom and Cablevision cases, the court concluded that it was Dish's subscribers, and not Dish itself, who were making the copies. The court considered the various ways in which Fox attempted to distinguish the facts at hand from the Cablevision case:

¹⁹⁷ Fox Broadcasting Co. v. Dish Network, L.C.C., 905 F. Supp. 2d 1088, 1093-95 (C.D. Cal. 2012), aff'd (as amended), 747 F.3d 1060 (9th Cir. 2014).

¹⁹⁸ Id. at 1096.

¹⁹⁹ Id. at 1097-98.

– Dish decided which networks were available on PTAT and defaulted the PTAT settings to record all four networks. Those decisions, while undoubtedly discretionary authority that Dish maintained, were similar to Cablevision’s unfettered discretion in selecting the programming available for recording. But Dish had no control over what programs Fox and the other networks chose to make available during primetime, and Dish recorded the programs only if the user made the initial decision to enable PTAT. The court concluded that the default settings did not support Fox’s contention that Dish, rather than its users, made the copies.

– Dish decided the length of time each copy was available for viewing before automatic deletion after a certain number of days and a user could neither delete nor preserve the original PTAT copy before that time. The court was not convinced, however, that this control, being exercised *after* the creation of the copies, was relevant to whether Dish caused the copies to be made in the first place, which were created only upon the users choosing to enable PTAT.

– Dish decided when primetime recordings started and ended each night and the user could not stop a copy from being made during the copying process, but had to wait until the recording ended before disabling the link to it on the hard drive. The court acknowledged that these limitations on user choice evinced Dish’s greater participation in the copying process, but nevertheless found that such involvement was not materially different from an Internet service provider that copied a file in automatic response to a user’s request, as in the Loopnet case. Although Dish defined some of the parameters of copyright for time-shifting purposes, it was ultimately the user who caused the copy to be made by enabling PTAT.

Accordingly, the court ruled that it was the user, not Dish, who was the most significant and important cause of the copy, and Fox had therefore not established a likelihood of success on the merits of its claim that by Dish directly infringed on its exclusive right to reproduction through PTAT.²⁰⁰

The court next ruled that Dish’s making of the QA copies did not constitute a fair use under the application of the four statutory fair use factors. Under the first factor, while the QA copies themselves were not sold or otherwise monetized, they were made for the commercial purpose of providing a high quality commercial skipping product that more users would want to activate. The copies were not transformative because they did not alter their originals with new expression, meaning or message. The first factor therefore weighed against fair use. The creative nature of the copyrighted works copied entitled them to heightened protection and cut against fair use under the second factor. The third factor also weighed against Dish because the entire works were copied, although the court noted that the third factor was of considerably less weight than the other factors due to the limited nature of the ultimate use.²⁰¹

Turning to the fourth factor, the court noted that the QA copies were used to perfect the functioning of AutoHop, a service that, standing alone, did not infringe. However, the record

²⁰⁰ Id. at 1099-1102.

²⁰¹ Id. at 1104.

showed that a market existed for the right to copy and use Fox programs, given that Fox licensed copies of its programs to companies including Hulu, Netflix, iTunes, and Amazon to offer viewers the Fox programs in various formats. In fact, the record suggested that Dish chose to offer AutoHop to its subscribers in order to compete with other providers who paid for the rights to use copies of the Fox programs through licensing agreements. By making an unauthorized copy for which it had not paid and using it for AutoHop, Dish harmed Fox's opportunity to negotiate a value for those copies and also inhibited Fox's ability to enter into similar licensing agreements with others in the future by making the copies less valuable. Therefore, the fourth factor also cut against Dish, and the court ruled that the QA copies did not constitute a fair use. The fact that consumers ultimately used AutoHop in conjunction with PTAT for private home use, a fair use under Sony, did not render the intermediate copies themselves a fair use as well.²⁰²

The court then considered whether Dish was liable for violation of Fox's distribution right and found that it was not. Citing the Perfect 10 v. Amazon case,²⁰³ the court noted that infringement of the distribution right requires actual dissemination of a copy by sale or other transfer of ownership, or by rental, lease, or lending. Here, a PTAT-enabled Hopper recorded primetime programming locally and, at most that local copy was disseminated within a single household. PTAT and AutoHop therefore did not involve any actual distribution of unauthorized copies, so the court concluded that Fox had not established a likelihood of success on the merits of its distribution claim.²⁰⁴

Lastly, the court turned to a consideration of whether a preliminary injunction should issue based on the court's finding that the QA copies were infringing.²⁰⁵ The court concluded that no preliminary injunction should issue because Fox had not established a likelihood of irreparable harm if Dish were not enjoined from making and using the QA copies. The record suggested that the extent of harm caused by the QA copies was calculable in money damages. The fact that Fox had licensing agreements with other companies showed that *copies* of the Fox programs had a market value that other companies already paid in exchange for the right to use the copies. Although Fox had submitted evidence that some irreparable harms, such as loss of control over its copyrighted works and loss of advertising revenue, might stem from the ad-skipping use to which the QA copies were put, the record did not show that those harms flowed from the QA copies themselves. Rather, if those harms were to materialize, they would be a result of the ad-skipping itself, which did not constitute copyright infringement. The court therefore concluded that any injury was compensable with money damages and did not support a finding of irreparable harm.²⁰⁶

²⁰² Id. at 1105-06.

²⁰³ Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1162 (9th Cir. 2007).

²⁰⁴ Fox Broadcasting, 905 F. Supp. 2d at 1106.

²⁰⁵ The court observed that "neither the marking announcements nor the ad-skipping effect of AutoHop implicates any copyright interest" Id. at 1110.

²⁰⁶ Id. at 1109-11.

On appeal, the Ninth Circuit affirmed.²⁰⁷ The Ninth Circuit expressly noted that direct infringement requires volitional conduct, by reciting that there are three elements to a prima facie case of direct infringement: (1) ownership of the allegedly infringed material, (2) violation of at least one exclusive right granted to copyright holders, and (3) volitional conduct by the defendant.²⁰⁸ It found that the district court did not abuse its discretion in determining that Fox was unlikely to succeed on its claim of direct copyright infringement regarding PTAT.²⁰⁹ “[O]perating a system used to make copies at the user’s command does not mean that the system operator, rather than the user, caused copies to be made. Here, Dish’s program creates the copy only in response to the user’s command. Therefore, the district court did not err in concluding that the user, not Dish, makes the copy.”²¹⁰ Citing Cablevision, the court noted the facts that Dish decided how long copies are available for viewing, modified the start and end times of the prime-time block, and prevented a user from stopping a recording might be relevant to a secondary or perhaps even a direct infringement claim, but they did not establish that Dish made the copies.²¹¹

The Ninth Circuit also determined that the district court did not abuse its discretion in concluding that Fox was unlikely to succeed on its claim of secondary copyright infringement for the PTAT and AutoHop programs because the activities of Dish’s users in making copies of Fox’s shows constituted fair use. The Ninth Circuit noted, as the district court held, that commercial skipping did not implicate Fox’s copyright interest because Fox owned the copyrights to the television programs, not to the ads aired in the commercial breaks.²¹² “If recording an entire copyrighted program is a fair use, the fact that viewers do not watch the ads not copyrighted by Fox cannot transform the recording into a copyright violation. ... Thus, any analysis of the market harm should exclude consideration of AutoHop because ad-skipping does not implicate Fox’s copyright interests.”²¹³

The Ninth Circuit found that Dish had demonstrated a likelihood of success on its customers’ fair use defense. With respect to the first factor, the court noted that Dish customers’ home viewing was noncommercial under Sony. Sony also governed the analysis of the second and third factors, by virtue of its holding that because time-shifting merely enables a viewer to see a work the viewer had been invited to witness in its entirety free of charge, the fact that the entire work is reproduced does not have its ordinary effect of militating against a finding of fair use. With respect to the fourth factor, the court noted that because Fox licenses its programs to distributors such as Hulu and Apple, the market harm analysis was somewhat

²⁰⁷ Fox Broadcasting Co., Inc. v. Dish Network L.L.C., 747 F.3d 1060 (9th Cir. 2014).

²⁰⁸ Id. at 1067.

²⁰⁹ Id. at 1066.

²¹⁰ Id. at 1067.

²¹¹ Id.

²¹² Id. at 1067-68.

²¹³ Id. at 1068.

different than in Sony, where no such secondary market existed for the copyright holders' programs. However, the court noted that the record before the district court established that the alleged market harm raised by Fox resulted from the automatic commercial skipping, not the recording of programs through PTAT. Specifically, it was the ease of skipping commercials, rather than the on-demand availability of Fox programs, that caused any market harm.²¹⁴

Finally, turning to the issue of Dish's direct infringement by making the QA copies, the Ninth Circuit ruled that the district court did not err in concluding that the QA copies were not a cause of Fox's alleged harm. That Dish used the copies in the process of implementing AutoHop did not suggest that those copies were integral to AutoHop's functioning. Rather, the record demonstrated that the AutoHop files containing the marking of commercials, which were the files distributed to users, were created using an entirely separate manual process and the QA copies were used only to test whether the marking process was working correctly. The Ninth Circuit also determined that the district court did not err in holding that monetary damages could compensate Fox for any losses from the QA copies. Accordingly, the Ninth Circuit concluded that the district court did not abuse its discretion in declining to grant Fox a preliminary injunction.²¹⁵

In Mar. 2014 Dish reached a settlement with the plaintiff Walt Disney Co. under which it agreed to disable the AutoHop function for ABC programming during the first three days after shows aired. In return Dish received the rights to stream content from ABC, ESPN and other Disney properties through a new, Internet-based TV service.²¹⁶

The Second Preliminary Injunction Ruling

On Feb. 21, 2013, Fox filed a first amended complaint and again sought a preliminary injunction against the following new functionalities that Dish had introduced in January of 2013 with its second generation Hopper DVR set-top box called "Hopper with Sling" that had Sling technology (which transcoded video content from its source at the DVR set-top box and transmitted it to remote devices over the Internet) built into the box itself:

-- Dish Anywhere, a mobile access application utilizing the Sling technology to allow subscribers to watch live television or television programs recorded on the Hopper from any location on remote devices connected to the Internet. No copies were made to facilitate the remote viewing via Dish Anywhere. The content was transferred via Internet directly from the

²¹⁴ Id. at 1068-69.

²¹⁵ Id. at 1072-73.

²¹⁶ Bill Donahue, "Dish, ABC Settle Ad-Skipping Fight with Broad TV Deal," *Law360* (Mar. 7, 2014), available as of Mar. 7, 2014 at www.law360.com/articles/515052/print?section=IP.

Hopper with Sling to the remote device and was not stored in and did not pass through any central server.²¹⁷

-- Hopper Transfers, which allowed Dish customers to copy pre-recorded programs from their DVRs to Apple iPad tablets (and later, other types of mobile devices) so they could be viewed on the go. An app paired the iPad (or other mobile device) with the customer's Hopper with Sling using the home wireless network, after which the customer could then use his or her home wireless network to copy recordings from the Hopper with Sling onto the iPad (or other mobile device). A Hopper Transfers-enabled device was required to reconnect via wireless Internet with the Hopper with Sling at least once every 30 days to verify the user's Dish subscription. If the device stayed disconnected for too long, the recordings stored on it were deleted.²¹⁸

The court denied the preliminary injunction on the grounds that Fox had not demonstrated irreparable harm. The court rejected the following bases that Fox asserted for irreparable harm:

-- Fox asserted that if Dish were allowed to offer the new services, other multi-channel video programming distributors (MVPDs) that competed with Dish and with whom Fox also had agreements would demand the same rights or other concessions to mitigate the risk of losing subscribers to Dish. The court found that Fox had presented no compelling evidence that other MVPDs would demand rights that were yet to be legally established rather than wait to see the result of the litigation before altering their contracts with Fox. And, because the new services were available only as an add-on to paid satellite television subscriptions, they did not threaten to diminish the value of the Fox programs. If Fox were to prevail on its claims, damages would be calculable.²¹⁹

-- Fox asserted it was likely to lose revenue from digital download services like Amazon.com and Apple iTunes, which Hopper Transfers threatened to supersede. The court rejected this argument, noting that Fox had not explained why its own digital download contracts with companies like Apple could not serve as benchmarks in calculating any damages caused by Hopper Transfers, were it found illegal. Nor had Fox refuted evidence that multi-screen live linear platform (MLLP) viewing enabled by Dish's new services increases viewership, and that historically, increased viewership can enhance viewer loyalty and increase revenue.²²⁰

-- Fox argued that Dish's services would cause it to lose one of its most important and valuable rights – the ability to control the timing and manner in which its copyrighted programs were distributed. The court rejected this argument, noting that the new services were available

²¹⁷ Fox Broadcasting Co. v. Dish Network, L.C.C., 2013 U.S. Dist. LEXIS 187499 at *2-7 (C.D. Cal. Sept. 23, 2013), aff'd, 583 Fed. Appx. 618 (9th Cir. 2014) (non-precedential).

²¹⁸ Id. at *8.

²¹⁹ Id. at *15-17.

²²⁰ Id. at *18-19.

only to preexisting Dish subscribers, and the fact that Fox and Dish already had a distribution agreement suggested that any loss of control could be readily remedied because the number of users was limited and ascertainable. In addition, the wide variety of similar services available to consumers would facilitate the calculation of damages, if necessary.²²¹

-- Fox also suggested irreparable harm from the fact that, because the new services were not authorized by Fox, they were not sufficiently protected from piracy and other online security risks. The court rejected this, noting that Sling hardware encrypted content to protect against piracy, and neither of the new services allowed users to make copies that could be duplicated or transferred beyond what was immediately authorized.²²²

-- Finally, Fox asserted that, because the new services would divert viewers from traditional viewing to Internet-based viewing (which tracking services like Nielsen were at that time unable to track), they would inhibit Fox's efforts to ascertain an accurate demographic profile of its audience, which would erode advertising value. The court rejected this, noting that although Nielsen did not currently track online viewing, it had announced that it would soon begin measuring viewership delivered through online connections. The court found Nielsen's announcement at least demonstrated that the trend in viewing practices was not going unnoticed, and it strongly suggested that the entities that gathered advertising data were ready and willing to adapt to the new landscape.²²³

On appeal, the Ninth Circuit affirmed in a brief, non-precedential opinion finding that the district court had committed no legal error and made no clearly erroneous factual findings in its denial of a preliminary injunction.²²⁴

The Rulings on Motion for Summary Judgment

After discovery, Fox moved for summary judgment on Fox's claims for direct copyright infringement.²²⁵ With respect to the PTAT service, the district court began by noting that the Ninth Circuit had upheld its earlier finding that the user, not Dish, made the PTAT copies. The district court noted that the current record reflected essentially the same facts about how PTAT worked and how much control Dish had over the process as it did at the preliminary injunction stage. Fox contended that the Supreme Court's Aereo decision (discussed in Section II.B.10 below) altered the test for direct infringement by rejecting the argument that only the subscriber who pushes the button initiating the infringing process is liable for direct infringement. The district court ruled, however (for the reasons discussed in Section II.B.16 below) that Aereo did not fundamentally alter the volitional conduct requirement for direct

²²¹ Id. at *19-20.

²²² Id. at *21-22.

²²³ Id. at *22-23.

²²⁴ Fox Broadcasting Co. v. Dish Network L.L.C., 583 Fed. Appx. 618 (9th Cir. 2014) (non-precedential).

²²⁵ Fox Broadcasting Co. v. Dish Network LLC, 160 F. Supp. 3d 1139, 1150 (C.D. Cal. 2015).

infringement. The court noted that, although more than one actor may be liable for direct infringement, there must still be some volitional conduct for direct liability. A system that operates automatically at a user's command to make a recording does not in itself render the system's provider a volitional actor for purposes of direct infringement. While Dish had set certain parameters and controls for PTAT, PTAT was essentially a more targeted version of a DVR that is set to make block recordings or recordings of an entire season of a show. The ability to set a DVR and then leave it to automatically record without having to select individual programs or set it repeatedly for each recording occasion was not unique to PTAT, and was not enough to show direct infringement by the service provider.²²⁶

A similar volitional conduct analysis applied to any direct infringement claim based upon "distribution." The court found that PTAT did not "distribute" Fox's programming because, as the court had previously held in its ruling on the first motion for a preliminary injunction, distribution under the copyright statute requires actual dissemination of a copy that changes hands. PTAT was a system for automatically recording programming as it was being received by a subscriber's set-top box, inside the subscriber's home. Those recordings were therefore not distributed, delivered, or transmitted to any other location or person using PTAT alone. The court also rejected Fox's argument that the mere "making available" of Fox's programming to subscribers was sufficient to constitute a distribution. The district court observed that, while neither the Ninth Circuit nor any other circuit court had addressed the "make available" theory of distribution under the copyright statute, it had been considered by a number of courts, and the great majority of courts that had considered the question had stopped short of fully endorsing the "make available" right. The district court found those cases persuasive and concluded that Dish's act of merely "making available" copyrighted programming to its subscribers through PTAT did not amount to distribution without actual dissemination.²²⁷

The court then turned to whether Dish could have secondary liability for PTAT use by Dish subscribers. To adjudicate that issue, the court had to determine whether such subscribers' use of PTAT constituted direct infringement or was a fair use. The court concluded that the subscribers' use of PTAT for time shifting was indeed a fair use. The court began by noting that the immunity of Sony is not absolute, and a challenge to a noncommercial use of a copyrighted work requires proof that either the particular use is harmful, or that if it should become widespread, there is some meaningful likelihood it would adversely affect the potential market for the copyrighted work. As of the time of the preliminary injunction request, the record established that any market harm resulted from the automatic commercial skipping and not simply the recording of programs through PTAT. However, at this later stage in the litigation, Fox had produced additional evidence of a secondary market for its programming. In addition to licensing the right to stream live its programming to certain MVPDs, Fox licensed third parties such as Apple, Amazon, Vudu and Microsoft the right to distribute its programs in a commercial-free, downloadable format, available the day after a program aired and viewable on mobile devices, personal computers, or certain Internet-connected televisions. Fox also licensed older

²²⁶ Id. at 1168-69.

²²⁷ Id. at 1169-70.

seasons of its programming to subscription video-on-demand services such as Netflix and Amazon Prime.²²⁸

The court therefore concluded that the record then before it established that a market for Fox programming on demand existed beyond the value of the advertisements. Nonetheless, the record did not create a triable issue as to the likelihood of future harm to that market. While Fox had provided some evidence that PTAT co-existed with services like Hulu that offered streaming of Fox programming with commercials, and that PTAT may help Dish attract subscribers, it had not demonstrated that any of this was genuinely likely to cause harm to the secondary market for Fox programming that went beyond the speculative, such that the question should be presented to a jury. Only Dish subscribers had access to PTAT, and those subscribers also had access to a litany of other services, including the ability to record prime time programming manually using more traditional DVR technology. Furthermore, PTAT recordings were available only for up to eight days, unless the subscriber made the effort to save them in a special folder for a longer period. Services that offered older seasons of Fox programming could not be in competition with recordings that were available only for up to eight days after a program aired. Similarly, the commercial-free programming Fox licensed to third parties was only potentially in competition with PTAT for up to eight days after a show aired, and then only for the group of people who both subscribed to Dish and used PTAT. Even in the unlikely event it were possible to demonstrate that Dish subscribers were less likely to purchase Fox programming on Amazon, or that potential Microsoft or Vudu customers would eschew those services in favor of Dish (which the record did not demonstrate beyond conjecture), it would be highly speculative and likely impossible to demonstrate that PTAT in particular, as opposed to other Dish features and services, would be the likely cause of market harm, or likely to be in the future. Accordingly, the court concluded that Dish subscribers' use of PTAT was fair use under Sony, and Dish was not liable for contributory infringement. The court therefore ruled that Dish did not directly or secondarily infringe Fox's right of reproduction or distribution by offering PTAT to its subscribers and therefore granted Dish summary judgment on those claims.²²⁹ (The court also ruled that Dish did not directly or secondarily infringe Fox's right of public performance by offering PTAT to its subscribers. See the discussion in Section II.B.16 below.)

The court then turned to whether Dish had direct liability for the QA copies of Fox programming that it made (until July 20, 2012) to ensure that AutoHop functioned properly on PTAT recordings made by Dish subscribers. Dish argued that the AutoHop service was non-infringing and the QA copies were fair use because they were intermediate copies that allowed for testing and development of new, non-infringing technology without affecting any licensing market in which Fox participated or reasonably would participate. In rebuttal, Fox first challenged whether AutoHop was infringing, arguing that the Ninth Circuit had upheld the ruling that it was not infringing on the ground that, if recording an entire copyrighted program was a fair use, the fact that viewers did not watch the ads not copyrighted by Fox could not transform the recording into a copyright violation. Since that ruling, Fox presented uncontroverted

²²⁸ Id. at 1170-71.

²²⁹ Id. at 1171-73.

evidence that it aired a significant number of commercials advertising its own programming, and that it owned copyrights for the clips used in those commercials. Fox argued that fact changed the analysis regarding whether AutoHop was non-infringing. The district court ruled, however, that it did not. The Ninth Circuit's observation was merely a point of emphasis to show how unlikely it would be for Fox to prevail on its claim that AutoHop infringed its copyrights – if Sony permits a consumer to record an entire copyrighted program under fair use, there could not be less protection for a consumer who declined to watch an ad that was not even copyrighted by Fox. The linchpin of the copyright infringement analysis was whether Dish had infringed Fox's rights of reproduction and distribution. AutoHop neither copied nor distributed anything – it *skipped* ads. Absent unauthorized copying or distribution, it was immaterial for purposes of the copyright infringement claim that the ads being skipped were Fox's own commercials.²³⁰

Nevertheless, the court reaffirmed its previous ruling from the preliminary injunction stage that creation of the QA copies was not a fair use. The QA copies were not transformative, because they were simply used to allow users to automatically skip commercials in the copyrighted programming rather than to create original programming or content. The QA copies in no way altered their originals with new expression, meaning or message. The commercial purpose of the QA copies weighed against fair use, as well as the creative nature of the copyrighted works. With respect to market harm, the court found the record reflected that there was a market for the right to copy and use Fox programs, given that Fox licensed copies of its programming to third parties like Hulu, Netflix and Amazon. Although there was no demonstrable existing market for the intermediate copies themselves, there was no material issue of disputed fact that Fox, as a normal course of business, monetized the right to copy its programming, whether directly (charging for the direct use of copies) or indirectly (allowing the use of copies as a part of a comprehensive licensing agreement). The fact that Dish's use of the QA copies was *sui generis* and had never been attempted before by any other entity did not, in the court's mind, mean that it had no intrinsic value. Accordingly, the court ruled that Dish's unauthorized use of QA copies would impair Fox's ability to monetize that use, not only as to Dish but also as to any other future technology creator that made analogous use of such copies, and thus did not constitute fair use.²³¹

The court therefore granted summary judgment in favor of Dish on the copyright infringement claim as to the AutoHop feature, and granted summary judgment in favor of Fox as to Dish's liability for direct infringement for creation of the QA copies.²³²

²³⁰ Id. at 1174-75.

²³¹ Id. at 1175-76.

²³² Id. at 1177. Fox sought statutory damages, compensatory damages in the form of reasonable royalties, and disgorgement of profits based on infringement by the QA copies. The court ruled that, although all such remedies are available under the copyright statute and potentially available if Fox prevailed at trial as to damages, it granted Dish's motion for summary judgment that Fox could not recover disgorgement of profits. The court noted that the QA copies facilitated one of the services that Dish offered its subscribers in order to convince them to subscribe. Fox had not demonstrated, however, that it could separate out Dish's profits that

Finally, the court turned to Fox's claims for direct and secondary liability of the reproduction right and the distribution right for offering the Hopper Transfers service. The court noted that Dish's control over the Hopper Transfers process was significantly less than its control over the PTAT process. Dish subscribers, not Dish, made and transferred the Hopper Transfers copies using Dish's equipment. Any potential distribution or performance was also by Dish subscribers, not Dish, so Dish was not liable for direct infringement by offering Hopper Transfers.²³³

Nor could Dish be secondarily liable because subscribers' creation of Hopper Transfers copies was a fair use. The court noted that Hopper Transfers was a technology that permitted non-commercial time shifting and place shifting of recordings already validly possessed by subscribers, which is paradigmatic fair use under existing law (citing the Ninth Circuit's Diamond Multimedia²³⁴ case).²³⁵ As with PTAT, where the subscriber engaged in the volitional conduct of copying, Fox had not demonstrated that Dish subscribers' use of Hopper Transfers standing alone was likely to cause harm to the secondary market for Fox programming that rose beyond the speculative, such that the question should be presented to a jury. Accordingly, subscribers' activation of Hopper Transfers was a fair use, and Dish was not liable for secondary infringement. The court therefore granted summary judgment in favor of Dish as to copyright infringement by Hopper Transfers.²³⁶

In February 2016, Fox and Dish reached a settlement. Dish agreed to turn off its DVR's ad-skipping function for the first seven days after broadcast, according to a joint statement. No further details of the agreement were made publicly available. This settlement followed earlier, similar settlements Dish had reached with Walt Disney Co., ABC, and CBS.²³⁷ In June 2016, Fox and NBC reached a settlement under which Dish agreed to turn off its DVR's ad-skipping function for the first seven days after broadcast. That settlement resolved the last remaining portion of the copyright litigation first instituted in 2012 by all four major networks over Dish's Hopper.²³⁸

flowed from the use of the AutoHop feature, let alone those that emanated solely from the limited-time use of the QA copies. Id. at 1181.

²³³ Id. at 1178.

²³⁴ Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., 180 F.3d 1072, 1079 (9th Cir. 1999).

²³⁵ Fox v. Dish, 160 F. Supp. 3d at 1178.

²³⁶ Id.

²³⁷ Bill Donahue, "Fox, Dish Settle Copyright Fight Over Ad-Skipping DVR," *Law360* (Feb. 11, 2016), available as of Feb. 11, 2016 at <http://www.law360.com/articles/758147>. In March of 2014, Walt Disney Co. and ABC had settled with Dish, dropping their similar lawsuits and giving Dish streaming right to ESPN in return for a three-day suspension of Hopper's ad-skipping feature. CBS struck a similar deal in December 2014, though it secured a seven day suspension of ad-skipping. Id.

²³⁸ Bill Donahue, "BNC, Dish Settlement Finally Ends Ad-Skipping DVR War," *Law360* (June 17, 2016), available as of June 20, 2016 at <http://www.law360.com/articles/808198>.

(v) Perfect 10 v. Giganews

The District Court Proceedings

In Perfect 10, Inc. v. Giganews, Inc.²³⁹ the defendants (Giganews and Livewire) were providers of access to USENET for a monthly fee starting at \$4.99 per month. The content posted by the defendants' subscribers and other USENET users, including infringing content, was stored on the defendants' servers. Before filing its complaint, the plaintiff sent a letter to one of the defendants, Giganews, notifying that it was infringing the plaintiff's copyrights, and included a DVD containing hundreds of Perfect 10 images, characterizing them as a sampling of its copyrighted materials that Giganews' site had offered for sale without authorization. Giganews responded by stating that each article posted on USENET has a unique message identification number, and if the plaintiff provided the identification numbers of the articles containing the infringing content, Giganews would be able to find the specific infringing material and remove it. The plaintiff did not do so. The plaintiff then filed a complaint for direct, contributory and vicarious copyright infringement and the defendants moved to dismiss all claims under Fed. R. Civ. Pro. 12(b)(6).²⁴⁰

With respect to the claims of copyright infringement, the court (Judge Matz) noted that the plaintiff's complaint was unclear as to the facts supporting those claims, but it appeared to be basing them on the following allegations: "(1) that Defendants are USENET providers who charge their subscribers a fee; (2) that Defendants program their computers to copy USENET content from other USENET servers and make this content available to their subscribers; (3) that USENET is now primarily used by its subscribers or visitors to exchange pirated content; (4) that Defendants are not only aware of the rampant piracy committed by USENET users but rely on the piracy as part of their business model; and (5) that Plaintiff has found at least 165,000 unauthorized Perfect 10 images on Defendants' USENET service."²⁴¹

The court then considered the volitional conduct requirement for direct infringement, noting that although the Ninth Circuit had not spoken on the issue, the Netcom principle that volitional conduct is required for direct liability had been widely accepted. The court noted, however, that the concept of "volitional" can be confusing, sometimes meaning "intentional," and yet no showing of intent is required for direct infringement liability.²⁴² "In this Court's view, the key to understanding the so-called 'volitional conduct' requirement is to equate it with the requirement of causation, not intent. 'Just who caused the copyright material to be infringed?' The Second Circuit's opinion in *Cartoon Network* is particularly helpful in this regard. In the words of that court, 'the question is *who* made this copy.'"²⁴³ The court cited the Cybernet

²³⁹ 2013 U.S. Dist. LEXIS 71349 (C.D. Cal. Mar. 8, 2013).

²⁴⁰ Id. at *1-7.

²⁴¹ Id. at *12-13.

²⁴² Id. at *16-17.

²⁴³ Id. at *17 (citations omitted).

Ventures and MAPHIA cases approvingly for their descriptions of the volitional conduct requirement as requiring that the defendant must “actively engage” or “directly cause” the infringing activity in order to be held liable for direct infringement.²⁴⁴

Applying these standards to the facts of the case, the court found that the plaintiff had not alleged that the defendants were the direct cause of, or actively engaged in, direct infringement. The plaintiff had alleged that the defendants copied all of the material on their servers from content uploaded onto USENET, stored these materials, most of which were infringing, on their servers, programmed their servers to distribute and download the infringing content, and controlled which materials were distributed to and copied from other third party servers. The court ruled that these facts did not indicate that it was the defendants themselves that committed the acts of copying, displaying or distributing the plaintiff’s copyrighted content and, as in Netcom, the defendants had merely engaged in the act of designing or implementing a system that automatically and uniformly created temporary copies of all data sent through it. Such conduct did not constitute a volitional act.²⁴⁵

Nor did the plaintiff’s allegations regarding the defendants’ knowledge of the pirated content on its servers salvage the plaintiff’s direct infringement claim. As the Netcom court pointed out, knowledge is not a required element of direct infringement, and the court ruled that a participant in the chain of events that ultimately allows viewers to obtain infringed material does not become the direct cause of the copying merely because he learned of it. The court noted that the Arista Records v. Usenet, MegaUpload, MP3tunes, and Playboy Enterprises cases had taken into account a defendant’s knowledge in determining whether that defendant engaged in volitional conduct, but disagreed with those decisions.²⁴⁶ “By focusing on the defendant’s awareness or state of mind – rather than on *who* actually caused the infringement – these cases effectively hold defendants liable for copyright infringement committed by third parties without requiring a full assessment of the additional elements of secondary copyright infringement claims.”²⁴⁷

Moreover, the court held the plaintiff’s allegation that the defendants controlled the content on their servers, without a good faith allegation specifying how the defendants exercised that control to directly create copies, could not alone create an inference that the defendants engaged in a volitional act directly causing infringement. Accordingly, the court dismissed the plaintiff’s claims for direct copyright infringement with leave to amend.²⁴⁸

The plaintiffs amended the complaint and the defendants again moved to dismiss. A different judge (Judge Collins) reaffirmed Judge Matz’s conclusion that the allegations did not

²⁴⁴ Id. at *18.

²⁴⁵ Id. at *21-22.

²⁴⁶ Id. at *22-25.

²⁴⁷ Id. at *25.

²⁴⁸ Id. at *22-23, *26.

support a claim for direct infringement against Giganews as a matter of law – because they mostly amounted to saying that Giganews programmed its servers to automatically copy, distribute, and display content uploaded by USENET users and/or at a user’s request, which did not amount to a volitional act²⁴⁹ – except that Judge Collins permitted Perfect 10’s claim for direct infringement against Giganews to proceed solely on the newly alleged theory that Giganews “plac[ed] copies of copyrighted material from various internet locations onto its own servers, and not at the request of customers ...”²⁵⁰ The amended complaint further alleged that, in view of how comprehensive, organized, and laborious the uploading of the plaintiff’s images had been, and in view of the financial benefit that Giganews reaped from the materials accessible to users through its server, it could be inferred that Giganews itself, through employees, uploaded some of the infringing materials. The court found this possibility to be rendered more plausible by the example of Megaupload, which the Dept. of Justice had recently found to have itself, and not at the request of users, uploaded massive quantities of copyrighted works to its own servers. Accordingly, the court concluded that the allegations that Giganews itself had uploaded the plaintiff’s copyrighted materials were sufficiently plausible to survive a motion to dismiss.²⁵¹

Judge Collins refused, however, to dismiss the claims of direct infringement against defendant Livewire, noting that, unlike Giganews, the material that Livewire made available to users was not posted on Livewire’s websites or servers by users. Rather, Livewire contracted with Giganews to obtain that content. However, because Livewire sold copies of that material to its customers, it had engaged in volitional conduct that could give rise to direct liability.²⁵²

After discovery, the defendants moved for partial summary judgment with respect to direct copyright liability. A third judge (Judge Birotte) granted the defendants’ motion.²⁵³ The court first turned to the question of whether there is a volitional requirement for direct liability. The court noted that the Ninth Circuit had not passed on Netcom’s causation analysis, although the court (inexplicably) did not cite the Ninth Circuit’s decision in Fox Broadcasting v. Dish Network (discussed in Section II.A.4(u) above), which did expressly adopt a volitional conduct requirement. The court noted some district court decisions in California that had not adopted the Netcom volitional conduct requirement, but declined to follow them. Although the court found the Netcom court’s passing use of the term “volition” to be somewhat confusing, as it might suggest a level of intent or willfulness that has no place in a claim for copyright infringement, the court found that the so-called “volition” element of direct infringement is not

²⁴⁹ Perfect 10, Inc. v. Giganews, Inc., 2013 U.S. Dist. LEXIS 98997 at *7-8 (C.D. Cal. July 10, 2013).

²⁵⁰ Id. at *7.

²⁵¹ Id. at *7-8. The court also dismissed Perfect 10’s allegation that Giganews directly infringed its display rights through the Mimo newsreader. The court noted that Mimo was just a reader, a piece of software that allowed a user to view an image. To the extent Mimo was used to view infringing images, that was done by the user. Furthermore, a user could use a number of other readers to view infringing content. That users might use Giganews’ reader to display infringing images did not constitute volitional conduct by Giganews. Id. at *6.

²⁵² Id. at *9.

²⁵³ Perfect 10, Inc. v. Giganews, Inc., 2014 U.S. Dist. LEXIS 183592 (C.D. Cal. Nov. 14, 2014).

a judicially-created element of intent or knowledge, but rather is a basic requirement of causation. Specifically, direct liability must be premised on conduct that can reasonably be described as the direct cause of the infringement with a nexus sufficiently close and causal to the illegal copying that one could conclude the alleged infringer himself trespassed on the exclusive domain of the copyright owner.²⁵⁴

Turning to each of the defendants separately, the court ruled with respect to Giganews that Perfect 10 could not prove causation for direct infringement as a matter of law. The court rejected Perfect 10's reliance on various cases that allegedly read the inaptly-named "volitional" conduct requirements as focusing on the defendant's awareness or state of mind, rather than on *who* actually caused the infringement. The court held that a claim of direct liability requires evidence that the defendants directly or actively caused the infringement, and Perfect 10's continued insistence that the defendants allowed their subscribers to upload, download, and view infringing material was the stuff of indirect or secondary liability, not direct liability. The court also found that Perfect 10 had failed to introduce any evidence on the single theory that Judge Collins had allowed to go forward – specifically, there was no evidence that Giganews' employees or agents themselves uploaded, downloaded, otherwise copied, displayed, or modified any work to which Perfect 10 held a copyright. All other bases on which Perfect 10 continued to allege direct liability had been previously rejected by both Judge Matz and Judge Collins, and Judge Birotte found no reason to depart from their previous analysis. After extensive discovery, the evidence before the court merely showed that Giganews offered its subscribers access to servers for a flat monthly fee, and there was no evidence that Giganews specifically sold access to Perfect 10 copyrighted materials as opposed to access to the entire USENET (of which Perfect 10 content was a fraction of a fraction), or even to erotic content in general.²⁵⁵

With respect to Livewire, the court found the evidence of direct infringement to be even more sparse. The sum total of evidence before the court was that Livewire paid Giganews to provide subscribers access to Giganews' USENET servers and, in turn, charged its subscribers a fee to access those servers. There was no evidence that Livewire operated any USENET servers of its own, or that any infringing material had ever appeared on any of the Web servers Livewire did own and operate. In denying Livewire's previous motion to dismiss Perfect 10's claim for direct infringement, Judge Collins had relied exclusively upon Perfect 10's allegation that Livewire sold the infringing material it received from Giganews at different prices, depending on usage. Despite extensive discovery, however, there was no evidence to support the allegation that Livewire sold any of Perfect 10's copyrighted material. Indeed, there was no evidence that Livewire even had a property interest in any of the content on Giganews' servers that Livewire was capable of selling.²⁵⁶

²⁵⁴ Id. at *22-26.

²⁵⁵ Id. at *29-34.

²⁵⁶ Id. at *34-38.

Accordingly, Judge Birotte granted partial summary judgment in favor of Giganews and Livewire on Perfect 10's claims of direct infringement. In addition, because Perfect 10's other theories of indirect liability as to Livewire had already been dismissed without leave to amend, the court ruled that its order completely disposed of all of Perfect 10's claims against Livewire. The court separately addressed Perfect 10's remaining claims for indirect liability as to Giganews in a separate order, granting partial summary judgment in favor of Giganews on those claims (see discussion in Section III.C.2(n) below).²⁵⁷

The Ninth Circuit's Decision

On appeal, the Ninth Circuit affirmed the district court's motion to dismiss and summary judgment rulings as to direct infringement. The court began by noting that direct infringement requires the plaintiff to show causation, also referred to as "volitional conduct," by the defendant. The court emphasized that the word "volition" in this context does not really mean an act of willing or choosing, or an act of deciding, as "volition" is defined in the dictionary. Rather, it is a requirement of proximate causation. The Ninth Circuit opined that this volitional conduct requirement is consistent with the Supreme Court's decision in Aereo, notwithstanding Justice Scalia's dissent in that case. The Aereo court did not expressly address the volitional conduct requirement for direct liability under the Copyright Act, nor did it directly dispute or comment on Justice Scalia's explanation of the doctrine. It would therefore be incorrect to presume that Aereo categorically jettisoned the doctrine by implication. Moreover, the Ninth Circuit opined that the Aereo court's analysis could be reconciled with the volitional conduct requirement in view of the fact that the Supreme Court distinguished between an entity that engages in activities like Aereo's and one that merely supplies equipment that allows others to perform or transmit, and further observed that a user's involvement in the operation of the provider's equipment and selection of the content transmitted might well bear on whether the provider performs within the meaning of the statute. Accordingly, the Ninth Circuit concluded that the volitional conduct requirement was left intact by Aereo and that the district court did not err in requiring Perfect 10 to satisfy it.²⁵⁸

Turning to Perfect 10's claims of direct infringement of its display right, Perfect 10 argued that its evidence showed Giganews was not merely a passive host, but rather directly caused the display of its images by making copies of those images and displaying them using its Mimo newsreader. As a preliminary matter, the Ninth Circuit noted that the district court concluded Perfect 10's display rights-based direct infringement claim failed at the pleadings stage. Thus, Perfect 10's argument on appeal that the district court ignored Perfect 10's evidence was irrelevant. Instead, the pertinent question was whether the first amended complaint alleged enough facts to state a claim to relief that was plausible on its face. The district court correctly concluded that the allegation that Giganews directly infringed Perfect 10's display rights through the Mimo reader did not state a claim because the allegation that users might use Giganews' reader to display infringing images did not constitute volitional conduct by Giganews. But even if

²⁵⁷ Id. at *43.

²⁵⁸ Perfect 10, Inc. v. Giganews, Inc., 847 F.3d 657, 666-67 (9th Cir. 2017).

the court were to consider Perfect 10's evidence, the Ninth Circuit ruled that its claim would still fail because that evidence showed only that Giganews' actions were akin to possibly storing material at the direction of users in order to make that material available to other users upon request, or automatically copying, storing and transmitting materials upon instigation by others. The Ninth Circuit therefore affirmed the district court's dismissal of Perfect 10's display rights-based direct infringement claim.²⁵⁹

Turning to Perfect 10's claim of direct infringement of its distribution right, the Ninth Circuit again noted that the district court had concluded Perfect 10's distribution rights-based theory as to Giganews failed at the pleadings stage. The district court had correctly held that the allegation that Giganews directly distributed Perfect 10's images when a user requested images from Giganews' servers did not state a claim because that distribution happened automatically, and Giganews had therefore not engaged in volitional conduct by which it caused the distribution. But again, the Ninth Circuit stated that even if it were to consider the evidence proffered by Perfect 10 as to Giganews, it would still conclude there was no direct infringement of Perfect 10's distribution right because Perfect 10 failed to show that the distribution did not happen automatically. With respect to Livewire, there was similarly no evidence that Livewire had any direct role in any act of infringement. There was no evidence indicating that distribution of Perfect 10's images did not happen automatically. The Ninth Circuit was unpersuaded by Perfect 10's argument that Livewire engaged in volitional conduct because it sold access to Giganews servers, including infringing Perfect 10 images, for a monthly fee. As the district court correctly concluded, the undisputed evidence showed Livewire sold access to all the content available on Giganews' servers, and there was no evidence that Livewire sold any of Perfect 10's copyrighted material. Accordingly, the Ninth Circuit affirmed the district court's rejection of Perfect 10's distribution rights-based direct infringement claims.²⁶⁰

Finally, turning to Perfect 10's claim of direct infringement of its reproduction right, Perfect 10 argued that it satisfied the volitional conduct requirement because Giganews itself instigated the copying, storage and distribution of Perfect 10's images. The Ninth Circuit rejected this argument, noting that Perfect 10 provided no evidence showing Giganews exercised control (other than by general operation of a Usenet service), selected any material for upload, download, transmission, or storage, or instigated any copying, storage or distribution. The court therefore affirmed the district court's holding that there was no triable issue of material fact as to Perfect 10's claim that Giganews directly infringed Perfect 10's reproduction right.²⁶¹

²⁵⁹ Id. at 668-69.

²⁶⁰ Id. at 669-70.

²⁶¹ Id. at 670.

(w) Capitol Records v. ReDigi

In Capitol Records, LLC v. ReDigi, Inc.,²⁶² ReDigi operated a web site that enabled users to “resell” their legally acquired iTunes music files and purchase “used” iTunes files from others at a fraction of the price on iTunes. To sell music on ReDigi’s web site, a user was required to download ReDigi’s “Media Manager” to his or her computer. Once installed, Media Manager analyzed the user’s computer to build a list of digital music files eligible for sale. A file was eligible only if it was purchased on iTunes or from another ReDigi user; music downloaded from a CD or other file-sharing web sites was ineligible for sale. After the validation process, Media Manager continually ran on the user’s computer and attached devices to ensure that the user had not retained music that had been sold or uploaded for sale. However, Media Manager could not detect copies stored in other locations. If a copy was detected, Media Manager prompted the user to delete the file. The file was not deleted automatically or involuntarily, although ReDigi’s policy was to suspend the accounts of users who refused to comply.²⁶³

Once uploaded, a digital music file underwent a second analysis to verify eligibility. If ReDigi determined that the file had not been tampered with or offered for sale by another user, the file was stored in ReDigi’s “Cloud Locker,” and the user was given the option of simply storing and streaming the file for personal use or offering it for sale in ReDigi’s marketplace. If a user chose to sell a digital music file, the user’s access to the file was terminated and transferred to the new owner at the time of purchase. When users purchased a file (at 59 cents to 79 cents), the seller received 20%, 20% went to an escrow fund for the artist, and 60% was retained by ReDigi. Capitol Records sued ReDigi for direct, contributory and vicarious copyright infringement.²⁶⁴

The court found ReDigi liable under all three theories. With respect to direct infringement, the court noted that courts had not previously addressed whether the unauthorized transfer of a digital music file over the Internet – where only one file exists before and after the transfer – constitutes reproduction within the meaning of the Copyright Act. The court held that it does. The court characterized the reproduction right as the exclusive right to embody, and to prevent others from embodying, a copyrighted work in a new material object. The court concluded that, because the reproduction right is necessarily implicated when a copyrighted work is embodied in a new material object, and because digital music files must be embodied in a new material object following their transfer over the Internet, the embodiment of a digital music file on a new hard disk is a reproduction within the meaning of the Copyright Act. The court determined this to be true regardless whether one or multiple copies of the file exist.²⁶⁵ “Simply put, it is the creation of a *new* material object and not an *additional*

²⁶² 934 F. Supp. 2d 640 (S.D.N.Y. 2013), aff’d, 910 F.3d 649 (2d Cir. 2018), cert. denied, 2019 U.S. LEXIS 4296 (June 24, 2019).

²⁶³ Id. at 645.

²⁶⁴ Id. at 646.

²⁶⁵ Id. at 648-50.

material object that defines the reproduction right.”²⁶⁶ The court found it to be beside the point that the original phonorecord no longer existed – it mattered only that a new phonorecord had been created.²⁶⁷

The court found sufficient volitional conduct on the part of ReDigi to hold it liable for direct infringement. The court noted that ReDigi’s founders had built a service where only copyrighted works could be sold. Media Manager scanned a user’s computer to build a list of eligible files that consisted solely of protected music purchased on iTunes. While the process was automated, absolving ReDigi of direct liability on that ground alone would be a distinction without a difference. The fact that ReDigi’s founders programmed their software to choose copyrighted content satisfied the volitional conduct requirement and rendered ReDigi’s case indistinguishable from those where human review of content gave rise to direct liability. Moreover, ReDigi provided the infrastructure for its users’ infringing sales and affirmatively brokered sales by connecting users who were seeking unavailable songs with potential sellers. The court concluded that such conduct transformed ReDigi from a passive provider of a space in which infringing activities happened to an active participant in the process of copyright infringement.²⁶⁸

Capitol Records also argued that ReDigi violated its distribution rights by simply “making available” Capitol Records’ recordings for sale to the public, regardless whether a sale occurred. The court cited a number of courts that had cast significant doubt on a “making available” theory of distribution,²⁶⁹ but concluded that because actual sales on ReDigi’s web site infringed Capitol Records’ distribution right, the court need not reach this additional theory of liability.²⁷⁰

The court found ReDigi contributorily liable because it knew or should have known that its service would encourage infringement, was aware that copyrighted content was being sold on its web site, and provided the site and facilities for the direct infringement. The court found that the site was, by virtue of its design to deal solely in music files from iTunes, not capable of substantial noninfringing uses. The court also ruled ReDigi to be vicariously liable because it exercised complete control over its web site content, user access, and sales, and benefitted financially from every infringing sale when it collected 60% of each transaction fee.²⁷¹ The court rejected ReDigi’s fair use defense because its web site made commercial use of the music files

²⁶⁶ Id. at 650 (emphasis in original).

²⁶⁷ Id.

²⁶⁸ Id. at 657.

²⁶⁹ Elektra Entertainment Group, Inc. v. Barker, 551 F. Supp. 2d 234, 243 (S.D.N.Y. 2008); London-Sire Records, Inc. v. John Doe 1, 542 F. Supp. 2d 153, 169 (D. Mass. 2008).

²⁷⁰ ReDigi, 934 F. Supp. 2d at 651 n.6.

²⁷¹ Id. at 658-60.

and did nothing to transform them, and ReDigi's sales were likely to undercut the market for or value of the copyrighted works.²⁷²

For the reasons set forth in Section III.F.1 below, the district court rejected ReDigi's assertion that the first sale doctrine permitted users to resell their digital music files on ReDigi's web site.

On appeal, the Second Circuit affirmed.²⁷³ The primary issue on appeal was whether ReDigi's system lawfully enabled resales of its users' digital files. The Second Circuit's rulings on that issue as well as the issue of fair use are described in Section III.F.1 below.

(x) Hearst Stations v. Aereo

This case was apparently the first one within the First Circuit to present the question whether a plaintiff claiming direct infringement must show volitional conduct on the part of the defendant. The court agreed with decisions in the Second, Third, and Fourth Circuits ruling that volitional conduct is required. The facts and rulings of this case are discussed in Section II.B.13 below.

(y) In Re Autohop Litigation (Dish Network v. American Broadcasting)

In In re Autohop Litigation,²⁷⁴ Dish Network brought a declaratory judgment action against several broadcasting companies seeking a declaration that its PrimeTime Anytime (PTAT) and AutoHop services (which are described in Section II.A.4(u) above) did not infringe the plaintiffs' copyrights. Several of the plaintiffs affiliated with ABC (including Disney) moved for a preliminary injunction preventing Dish from offering its PTAT and AutoHop services to its subscribers. The plaintiffs argued that Dish was liable for directly infringing their copyrights in their primetime programs by virtue of its involvement in creating the key system settings and options subscribers could choose for recording broadcasts via PTAT. The plaintiffs argued that Dish did not simply and automatically obey subscriber commands because the start and stop times of recordings were set by Dish and Dish prevented a subscriber from stopping a recording once it was in progress. The plaintiffs pointed out that Dish did not limit the copying to the programs that the subscriber intended to watch and argued that Dish had control over the content of the programming because its agents allegedly consulted an electronic program guide to determine which programs fell into primetime and which should be recorded.²⁷⁵

²⁷² Id. at 653-54.

²⁷³ Capitol Records, LLC v. ReDigi Inc., 910 F.3d 649 (9th Cir. 2018), cert. denied, 2019 U.S. LEXIS 4296 June 24, 2019.

²⁷⁴ 2013 U.S. Dist. LEXIS 143492 (S.D.N.Y. Oct. 1, 2013). The opinion states in its caption that it is related to Dish Network, L.L.C. v. American Broadcasting Cos.

²⁷⁵ Id. at *1-2, *16-19.

The district court found it unnecessary to resolve the disputed question of whether the primetime programming was identified through the operation of software or through human review of program schedules because under the Second Circuit's Cartoon Network (Cablevision) case, the pivotal factor for direct liability is initiation of the act of copying rather than the selection of offerings for possible copying or the creation of the technological structure. The possible involvement of Dish's agents in determining the time parameters of programming available for PTAT/Hopper recording was therefore insufficient to render Dish a direct infringer. The court noted that Dish had no control over which programs would be shown on the plaintiffs' networks or in what order, just as it had no control over which of its subscribers would choose to copy those programs. It was the Dish subscriber who decided if he or she wanted to use the PTAT feature and the subscriber was required to enable PTAT before the Hopper would record any programs. The subscriber also selected which of the networks' primetime offerings to record and which nights to record and, once the subscriber enabled the PTAT, the recordings were saved on the subscriber's personal hard drive on the Hopper, rather than at Dish headquarters. The subscriber also decided the length of time the recordings should be kept. Accordingly, the court ruled that the subscribers made the copies, and the plaintiffs had therefore failed to demonstrate a likelihood of success on a claim for direct infringement liability.²⁷⁶

The court also ruled that Dish had no secondary liability for its subscribers' copying under either vicarious or contributory theories. With respect to vicarious liability, the court found that Dish had no control over whether its subscribers enabled the PTAT technology or what they chose to copy. The court also concluded that Dish was likely to establish that it could have no secondary liability under the Sony case because the copying by Dish's subscribers for private, non-commercial time shifting use in the home was a fair use. Accordingly, the court denied the plaintiffs' request for a preliminary injunction.²⁷⁷

In Mar. 2014 Dish reached a settlement with the plaintiff Walt Disney Co. under which it agreed to disable the AutoHop function for ABC programming during the first three days after

²⁷⁶ Id. at *19-21.

²⁷⁷ Id. at *22-26, *48. The court also found that the plaintiffs had failed to establish irreparable harm. The plaintiffs argued they would suffer irreparable harm because AutoHop's efficient commercial skipping feature would deprive them of advertising revenues premised on PTAT/AutoHop commercial viewing patterns, such as live TV-watching, commercial-inclusive VOD without fast-forwarding ability, and Hulu, which all exposed viewers to opportunities to watch commercials during primetime programming, thus harming the plaintiffs' relationships and negotiations with authorized licensees. The court found, however, that the plaintiffs had not proffered any evidence of actual and imminent injury. The court noted that Nielsen's C3 rating system did not distinguish between commercial-skipping using AutoHop and commercial skipping using other, preexisting technologies, instead measuring only whether the commercial had been skipped or not. The record therefore did not support the conclusion that there would likely be an incremental increase in commercial skipping from AutoHop. In fact, the plaintiffs' corporate designee and expert on consumer behavior had testified that DVRs in general had actually boosted the C3 ratings of its programming. Id. at *30-31.

shows aired. In return Dish received the rights to stream content from ABC, ESPN and other Disney properties through a new, Internet-based TV service.²⁷⁸

(z) Oppenheimer v. Allvoices

In this case, the plaintiff brought claims for copyright infringement for unlicensed use of his photographs on the defendant Allvoices' web site. Allvoices was an online service provider that operated a web site set up as a community for its users to share and discuss news, by contributing related text, video and images, and commenting. Citizen journalists who posted news, videos, images and commentary were paid consideration for their article contributions based on the popularity of, and web traffic to, their articles. Allvoices filed a motion to dismiss the plaintiff's direct infringement claim on the basis that it could not have direct liability under the volitional conduct requirement. The court noted that, although the Netcom requirement of volitional conduct for direct liability had been adopted by the Second and Fourth Circuits, the Ninth Circuit had not yet addressed the issue, and district courts within the Ninth Circuit were split on the issue. But even if a direct copyright infringement claim requires a plaintiff to allege that the defendant engaged in volitional conduct that caused the infringement, the court found the plaintiff had done so. Contrary to Allvoices' suggestion, the plaintiff had not alleged that contributors infringed the plaintiff's photographs on their own by uploading them onto Allvoices. Rather, the plaintiff's first amended complaint alleged that Allvoices, both directly and through contributors, reproduced and displayed the photographs without the plaintiff's permission. Such allegations were sufficient to deny the defendant's motion to dismiss the direct infringement claim.²⁷⁹

(aa) The Supreme Court's Aereo Decision

Although the Supreme Court's majority opinion in American Broadcasting Co. v. Aereo, Inc.²⁸⁰ did not address the volitional conduct requirement in copyright law, a strong dissenting opinion by Justice Scalia articulated the position that the volitional conduct doctrine, though not ever addressed expressly by the Supreme Court, had become well established in the appellate courts, was consistent with Supreme Court precedent, and Aereo could not be found to have "performed" the works at issue by virtue of that doctrine. See the discussion of the case in Section II.B.10 below.

(bb) Gardner v. CafePress

The case of Gardner v. CafePress Inc.²⁸¹ was the first case decided after the Supreme Court's Aereo decision to rule that Aereo did not eliminate the volitional conduct requirement

²⁷⁸ Bill Donahue, "Dish, ABC Settle Ad-Skipping Fight with Broad TV Deal," *Law360* (Mar. 7, 2014), available as of Mar. 7, 2014 at www.law360.com/articles/515052/print?section=IP.

²⁷⁹ Oppenheimer v. Allvoices, Inc., 2014 U.S. Dist. LEXIS 80320 at *1-2, *19-22 (N.D. Cal. June 10, 2014).

²⁸⁰ 134 S. Ct. 2498, 2504 (2014).

²⁸¹ 2014 U.S. Dist. LEXIS 168328 (S.D. Cal. Dec. 4, 2014).

for direct liability. CafePress operated an e-commerce site that allowed users to upload images of artwork, slogans and designs for printing by CafePress on items such as shirts, bags and mugs. The images were uploaded at the direction of CafePress users and were stored on CafePress's servers through its web site. CafePress users could also offer the uploaded images for sale to third parties who then selected one of CafePress's unbranded items on which to print the images. Several CafePress users uploaded copies of the plaintiff's works to CafePress's service without permission and then sold items bearing copies of the plaintiff's works through CafePress's web site and other web sites. CafePress received revenue from these infringing sales. CafePress also purchased advertisements which displayed copies of the plaintiff's works and generated revenue from users who clicked on those advertisements. The plaintiff brought claims for direct and vicarious copyright liability against CafePress and CafePress sought summary judgment in its favor on liability.²⁸²

With respect to direct liability, the plaintiff argued that the Supreme Court's decision in Aereo militated against a volitional conduct requirement for direct liability. The district court rejected this argument, noting that the Supreme Court expressly decided not to address the volitional conduct issue, which therefore left undisturbed the Ninth Circuit's decision in Fox Broadcasting Co. v. Dish Network L.L.C.,²⁸³ which expressly held that volitional conduct on the part of the defendant is one of three elements required to establish a prima facie case of direct infringement. Here the court found volitional conduct on the part of CafePress sufficient for direct liability in the form of the production and sale of allegedly infringing items bearing the plaintiff's copyrighted images. CafePress did not contend that its production facility and shipping processes were completely automated and thus devoid of human employees engaging in volitional conduct. Rather, CafePress's employees responded to customer requests to purchase items by operating the machinery used to create the allegedly infringing items.²⁸⁴

With respect to vicarious liability, the court found direct financial benefit from the infringing activity on the part of CafePress because it was undisputed that a certain number of CafePress customers saw ads bearing images of the plaintiff's copyrighted works, clicked through those ads, and generated revenue for CafePress, and that some CafePress customers bought items bearing images of the plaintiff's copyrighted works. The court also found the evidence showed that CafePress had active control over at least some of the allegedly infringing items during the process in which CafePress produced and then shipped those items to customers.²⁸⁵ "While CafePress's actions in response to allegedly infringing uploads may be similar to Amazon and eBay where it is not actively involved and can only engage in after-the-fact removal and access blocking, CafePress's production of allegedly infringing items at its production facility does appear to be 'purposeful conduct' such that CafePress has the 'right and ability to control.'"²⁸⁶

²⁸² Id. at *1-4. The plaintiff did not assert claims for contributory liability.

²⁸³ 747 F.3d 1060 (9th Cir. 2014).

²⁸⁴ CafePress, 2014 U.S. Dist. LEXIS 168328 at *8-12.

²⁸⁵ Id. at *13-16.

²⁸⁶ Id. at *16.

Accordingly, the court denied CafePress’s motion for summary judgment in its favor with respect to liability for direct and vicarious infringement.²⁸⁷

(cc) Rosen v. eBay

In this case, the plaintiff Rosen was the owner of copyrights in several photographs. He sought to hold eBay liable for copyright infringement based on the offering for sale of unauthorized copies of his photographs through the eBay marketplace. Rosen alleged eBay had committed direct copyright infringement based on the fact that, in creating the listings on its marketplace, eBay created a copy of his copyrighted photos and stored it on eBay’s servers. The court denied liability for direct infringement on the ground that a third party’s infringing use of a defendant’s automated system does not render the defendant directly liable. Accordingly, eBay could not be a direct infringer as a result of its users putting his photos on eBay’s servers and making them publicly available.²⁸⁸

(dd) BWP Media v. T&S Software

In this case, the defendant, an Internet service provider, hosted a public forum called “HairTalk” on which third party users posted images that infringed copyrights owned by the plaintiffs. The plaintiffs sued for direct and secondary copyright infringement. The district court granted summary judgment in favor of the defendant. The plaintiffs appealed only the district court’s direct infringement holding. The Fifth Circuit affirmed, adopting the volitional conduct requirement in direct copyright infringement cases.²⁸⁹

During the relevant time period, the defendant did not have an agent designated to receive notices of content that should be removed from its site, so it was not entitled to the DMCA safe harbor under Section 512(c). The court therefore noted that the determinative issue on appeal was whether volitional conduct is required to prove a claim of direct infringement, an issue that had apparently not previously been decided by the Fifth Circuit. The court began by noting that every Circuit to address the issue had adopted some version of the volitional conduct requirement.²⁹⁰ The court further noted that the word “volition” in this context does not really mean an act of willing or choosing or deciding, but rather one of proximate causation.²⁹¹

The plaintiffs argued that the court should not follow the previous Circuit decisions because the Supreme Court’s 2014 decision in Aereo had supposedly rejected both the Netcom

²⁸⁷ Id. at *18.

²⁸⁸ Rosen v. eBay, Inc., 2015 U.S. Dist. LEXIS 49999 at *2, *14-16 (C.D. Cal. Jan. 16, 2015).

²⁸⁹ BWP Media USA, Inc. v. T&S Software Assocs., Inc., 852 F.3d 436, 438, 444 (5th Cir. 2017), cert. denied, 2017 U.S. LEXIS 5813 (Oct. 2, 2017).

²⁹⁰ The court cited Perfect 10, Inc. v. Giganews, Inc., 847 F.3d 657, 666-67 (9th Cir. 2017); Leonard v. Stemtech Int’l Inc., 834 F.3d 376, 387 (3d Cir. 2016); and Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121, 131 (2d Cir. 2008).

²⁹¹ BWP Media, 852 F.3d at 438-40 & n.1.

line of cases and the volitional conduct requirement. The Fifth Circuit rejected this argument, finding that the Supreme Court never addressed whether Aereo's conduct was volitional, resting its holding instead on the similarities between cable TV systems and Aereo's system, and had in fact left open the question whether, in cases involving different kinds of service or technology providers, a user's involvement in the operation of the provider's equipment and selection of the content transmitted might bear on whether the provider performed within the meaning of the copyright act. The Fifth Circuit therefore agreed with the Ninth Circuit's Giganeews decision that the volitional conduct requirement is consistent with the Aereo majority opinion.²⁹²

With respect to the case at hand, the Fifth Circuit found the facts to be much closer to those in the Netcom line of cases than those in Aereo. Although Aereo and the defendant here both provided a service that others could use to infringe, only Aereo played an active role in the infringement by routing infringing content to its users. The same could not be said of the defendant's conduct. Although the defendant hosted the forum on which infringing content was posted, its connection to the infringement ended there. Unlike Aereo, the defendant did not provide users with access to the content, so that the defendant and the infringing conduct were not linked by volitional conduct.²⁹³

The plaintiffs also argued that the safe harbor rules of Section 512(c) created the exclusive method of protecting an arguably innocent service provider. The plaintiffs argued that adopting the volitional conduct requirement would render Section 512(c)'s safe harbor meaningless and would disincentivize DMCA compliance by benefitting those ISPs that choose not to satisfy Section 512(c)'s requirements. The court rejected this argument for the same reasons that the Fourth Circuit had previously done so in the CoStar case. The Fourth Circuit found that the argument was belied by the plain language of the DMCA itself in Section 512(l), which provides that the DMCA does not bear adversely upon any of a service provider's other defenses under law to an infringement claim. The Fifth Circuit therefore agreed with the Fourth Circuit's conclusion in CoStar that the DMCA's safe harbor for service providers is a floor, not a ceiling, of protection. Rather than altering the volitional conduct requirement, the DMCA merely added a second step to assessing infringement liability for service providers after a determination whether it is an infringer in the first place.²⁹⁴ Finally, the Fifth Circuit rejected the plaintiffs' argument that retaining the volitional conduct requirement diminishes Section 512(c)'s usefulness in direct infringement cases. The court noted that may be, but it does not do so in secondary infringement cases. According, the court adopted the volitional conduct requirement in direct copyright infringement cases. Because the plaintiffs did not contend that the defendant did, in fact, engage in such conduct, the court affirmed the district court's grant of summary judgment.²⁹⁵

²⁹² Id. at 440-42.

²⁹³ Id. at 442.

²⁹⁴ Id. at 442-43 (citing CoStar Grp., Inc. v. LoopNet, Inc., 373 F.3d 544, 552, 555 (4th Cir. 2004)).

²⁹⁵ BWP Media, 852 F.3d at 444.

(ee) **Williams-Sonoma v. Amazon.com**

Amazon operated an online marketplace on Amazon.com in which sellers could offer items for sale, including peppermint bark candy and other branded products from the plaintiff Williams-Sonoma, Inc. (WSI). WSI did not sell or authorize the resale of its products on Amazon.com nor did it authorize the use of its copyrighted photos on the Amazon platform. The products sold on Amazon.com were showcased on Amazon-generated listing pages called “product detail pages” or “PDPs.” Amazon did not allow its sellers to make their own listings for each product they wanted to sell. Instead, it forced all sellers who were offering the same product to share a single PDP.²⁹⁶

The complaint alleged that Amazon asserted systematic and exclusive control over every aspect of its PDPs. It solicited the content for its PDPs from marketplace sellers, who could submit proposed images and verbiage for potential inclusion on a PDP pursuant to Amazon’s comprehensive guidelines detailing how to draft the content for the pages, what could and could not be included, and what kinds of images to submit. Sellers could not upload photos or verbiage directly to a PDP – instead, Amazon collected the content submitted by its sellers into an internal database it called its “catalog.” From there, Amazon used multiple algorithms to evaluate and select the seller-contributed content for a wide variety of aspects of its product listings, including images. Amazon maintained sole discretion over what images and content were chosen from its catalog to display publicly on its PDPs. When multiple images existed for a product, Amazon, using its algorithms, selected which product image, among other elements, was mostly likely to make the sale and displayed that image on the PDP for the product. WSI alleged that this multi-factor selection constituted a positive selection process that was tantamount to an employee exercising editorial control, thereby making Amazon liable as a direct infringer for the unauthorized display of WSI photos on the Amazon web site – specifically, the PDP for WSI’s Original Peppermint Bark 2lb Tin, which displayed WSI’s copyrighted Peppermint Bark Photo without WSI’s permission. Amazon moved to dismiss the direct infringement claim.²⁹⁷

The court found Amazon’s characterization of its selection process as one of automatic blocking, screening or gatekeeping to be inconsistent with WSI’s factual allegations which must be accepted as true at the pleading stage. Those allegations supported the reasonable inference that when multiple sellers uploaded proposed photos for the same product, Amazon’s image-selection algorithm affirmatively selected the image that it deemed most likely to make the sale, and thus Amazon made an editorial, qualitative decision among different photos of the same product, regardless of any rights to do so, and then copied and displayed the chosen image using multi-factor criteria designed and employed by Amazon. As further alleged by WSI, Amazon’s system thereby picked the most attractive photos irrespective of rights, which enhanced rather

²⁹⁶ Williams-Sonoma, Inc. v. Amazon.com, Inc., 2020 U.S. Dist. LEXIS 163066 at *4-5 (N.D. Cal. Aug. 17, 2020).

²⁹⁷

than reduced the potential for infringement of professionally produced photographs. The court therefore ruled that these allegations adequately supported WSI's assertion that Amazon exercised the requisite level of volition necessary to be held liable as a direct infringer of SWI's reproduction and public display rights.²⁹⁸

As an independent basis for dismissal, Amazon asserted the Section 512(c) safe harbor on the ground that WSI's copyrighted photos were stored at the direction of Amazon's users. The court refused to dismiss on that basis as well, ruling that the complaint alleged factual matters regarding Amazon's role in the reproduction and display of WSI's copyrighted images that could refute its ability to establish that the photos were stored at the direction of its users. The complaint also alleged specific facts that tended to refute other required elements of the Section 512(c) safe harbor – namely, that Amazon did not have the right and ability to control the infringing activity, and did not financially benefit from the infringement (the court noted allegations that Amazon took a cut on every sale transaction).²⁹⁹

(ff) Summary of Case Law

To sum up, under a majority of the cases, a direct volitional act of some kind is required for liability for direct copyright infringement. The MAPHIA and Sabella, Cablevision, and Hotfile cases suggest that it is insufficient for direct liability for an actor such as a BBS or web site operator to have provided only encouragement of the acts (such as initial uploading of unauthorized copies) that lead to infringement. Similarly, the CoStar, Ellison and Perfect 10 v. Cybernet Ventures cases suggest that an OSP will not have direct liability for infringing material posted on its service by users or available through its service on third party sites where the OSP has not encouraged such posting or had advance knowledge of it. And the Field v. Google and Parker v. Google cases hold that a search engine operator will not have direct liability for serving up cached copies of copyrighted materials in an automated response to user requests based on search results. Rather, for direct liability the defendant must have engaged in the very acts of infringement themselves in a volitional way. The Perfect 10 v. Giganews case, while agreeing with Netcom that a volitional act is required for direct infringement, equated the “volitional conduct” requirement with a requirement of causation, not intent. That court cited the Cybernet Ventures and MAPHIA cases approvingly for their descriptions of the volitional conduct requirement as requiring that the defendant must “actively engage” or “directly cause” the infringing activity in order to be held liable for direct infringement.

However, the Frena, Webbworld, Sanfilippo, Quantum Systems, Megaupload and ReDigi cases (as well as the Hardenburgh and Webbworld cases discussed in Section II.C below with respect to the public display and distribution rights) suggest that where an actor such as a BBS operator or web site operator has some form of substantial direct involvement in the anticipated acts that lead to infringement or in the infringing acts themselves (such as resale of the infringing material), there may be a finding of sufficient volitional activity to impose direct liability. And the

²⁹⁸ Id. at *16-19.

²⁹⁹ Id. at *20-22.

Arista Records v. Usenet.com case suggests that direct liability for violation of the distribution right can be premised on active promotion of sharing of illicit files coupled with close control over what types of material are featured for distribution in the first instance. Thus, to establish direct liability for infringement one must look at whether the defendant participated in the very acts of infringement themselves.

One district court case – the Myxer case – simply refused to adopt the volitional requirement for direct infringement, noting that the Ninth Circuit had never expressly adopted the volitional requirement and finding such a requirement to be inconsistent with copyright infringement being a strict liability tort. The Ninth Circuit subsequently did, however, expressly adopt the volitional requirement in the 2014 Fox Broadcasting v. Dish Network case.

As discussed in Section III.C below, the Digital Millennium Copyright Act³⁰⁰ (referred to herein as the “DMCA”) defines certain safe harbors against liability for OSPs who act as merely passive conduits for infringing information and without knowledge of the infringement. An OSP must meet quite specific detailed requirements to qualify for the safe harbors relating to acting as a passive conduit and innocent storage of infringing information. Where an OSP does not qualify for these safe harbors, the standards under the case law discussed above will apply to determine liability.

5. The Reproduction Right Under WIPO Implementing Legislation

(a) United States Legislation

Four bills were introduced in Congress to implement the WIPO treaties. Two of them, neither of which were ultimately enacted, would have attempted to clarify the issue of whether interim copies made during the course of transmission infringe the reproduction right. The bill that was adopted – The Digital Millennium Copyright Act – contains nothing explicitly addressing the scope of the reproduction right in a digital environment.

(1) The Digital Millennium Copyright Act

The DMCA was signed into law by President Clinton on Oct. 28, 1998. It is essentially an enactment of H.R. 2281, introduced in the House in July of 1997 by Rep. Howard Coble, and its nearly identical counterpart in the Senate, S. 1121, introduced by Sen. Orrin Hatch also in July of 1997, which was later combined with another bill and, as combined, denominated S. 2037. Both H.R. 2281 and S. 1121 were introduced with the support of the Clinton administration.

Title I of the DMCA, entitled the “WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998” and comprised of Sections 101 through 105, implements the WIPO treaties. Title I takes a minimalist approach to implementing the requirements of the WIPO treaties. The Clinton administration took the view that most of the enhanced copyright

³⁰⁰ Pub. L. No. 105-304, 112 Stat. 2860 (1998).

protections set forth in the treaties were already available under United States law, so that no major changes to U.S. law were believed necessary to implement the treaties.

Specifically, the DMCA addresses only the requirements of Arts. 11 and 12 of the WIPO Copyright Treaty, and of Arts. 18 and 19 of the WIPO Performances and Phonograms Treaty, to provide adequate legal protection and effective legal remedies against (i) the circumvention of effective technological measures that are used by rights holders to restrict unauthorized acts with respect to their protected works, and (ii) the removal or alteration of any electronic rights management information (information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work), or the distribution or communication to the public of copies of works knowing that the electronic rights management information has been removed or altered. The specific provisions of these bills are discussed in further detail below. These bills contain nothing addressing the reproduction right or how that right relates to the digital environment.

(2) Legislation Not Adopted

An alternative bill to implement the WIPO treaties, S. 1146, entitled the “Digital Copyright Clarification and Technology Education Act of 1997,” was introduced on Sept. 3, 1997 by Sen. John Ashcroft. Like the DMCA, S. 1146 contained language to implement prohibitions against the circumvention of technologies to prevent unauthorized access to copyrighted works and to provide electronic rights management information about a work, although it adopted a different approach to doing so than the DMCA, as discussed further below.

S. 1146 also contained, however, a much broader package of copyright-related measures. With respect to the reproduction right, S. 1146 would have clarified that ephemeral copies of a work in digital form that are incidental to the operation of a device in the ordinary course of lawful use of the work do not infringe the reproduction right. Specifically, S. 1146 would have added a new subsection (b) to Section 117 of the copyright statute to read as follows:

(b) Notwithstanding the provisions of section 106, it is not an infringement to make a copy of a work in a digital format if such copying –

(1) is incidental to the operation of a device in the course of the use of a work otherwise lawful under this title; and

(2) does not conflict with the normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author.

The proposed new clause (b)(1) was similar to the right granted in the existing Section 117 of the copyright statute with respect to computer programs, which permits the making of copies of the program “as an essential step in the utilization of the computer program in conjunction with a machine.”³⁰¹ Clause (b)(1) would have extended this right to the otherwise

³⁰¹ 17 U.S.C. § 117.

lawful use of other types of works in a digital format, to the extent that copying is necessary for such use. It would seem to have covered activities such as the loading of a musical work into memory in conjunction with playing the work, the incidental copies of a movie or other work ordered on demand that are made in memory in the course of the downloading and viewing of the movie, and the various interim copies of a work that are made in node computers in the routine course of an authorized transmission of the work through the Internet.

The limiting language contained in new clause (b)(2) was drawn directly from the WIPO treaties themselves. Specifically, Article 10 of the WIPO Copyright Treaty permits treaty signatories to provide for limitations of or exceptions to the rights granted under the treaty “in certain special cases that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the author.” The scope of reach of this language is obviously not self evident, and the boundaries of this exception to the reproduction right are therefore not entirely clear. However, the exception should apply to at least the most common instances in which incidental copies must be made in the course of an authorized use of a digital work, including in the course of an authorized transmission of that work through a network.

Another bill introduced into Congress to implement the WIPO copyright treaties was H.R. 3048, entitled the “Digital Era Copyright Enhancement Act,” which was introduced on Nov. 14, 1997 by Rep. Rick Boucher. With respect to the reproduction right, H.R. 3048 contained an identical amendment to Section 117 as S. 1146 that would have permitted the making of incidental copies of a work in digital form in conjunction with the operation of a device in the ordinary course of lawful use of the work.

The clarifying amendment to Section 117 concerning the reproduction right that these alternative bills would have set up was not ultimately adopted by Congress in the DMCA.

(b) The European Copyright Directive

The European Copyright Directive contains strong statements of copyright owners’ rights to control the reproduction, distribution and presentation of their works online. The European Copyright Directive requires legislative action by EC member states with respect to four rights: the reproduction right,³⁰² the communication to the public right,³⁰³ the distribution right,³⁰⁴ and protection against the circumvention or abuse of electronic management and protection systems.³⁰⁵

With respect to the reproduction right, the European Copyright Directive adopts essentially the same broad language of proposed Article 7(1) of the WIPO Copyright Treaty that

³⁰² European Copyright Directive, art. 2.

³⁰³ *Id.* art. 3.

³⁰⁴ *Id.* art. 4.

³⁰⁵ *Id.* arts. 6-7.

provoked so much controversy and was ultimately deleted from the WIPO Copyright Treaty. Specifically, Article 2 of the European Copyright Directive provides that member states must “provide the exclusive right to authorize or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form” of copyrighted works. The extension of the reproduction right to “direct or indirect” and “temporary or permanent” reproductions would seem to cover even ephemeral copies of a work made during the course of transmission or use of a copyrighted work in an online context. Indeed, the official commentary to Article 2 notes that the definition of the reproduction right covers “all relevant acts of reproduction, whether on-line or off-line, in material or immaterial form.”³⁰⁶ The commentary also appears to adopt the approach of the MAI case in recognizing copies of a work in RAM as falling within the reproduction right: “The result of a reproduction may be a tangible permanent copy, like a book, but it may just as well be a non-visible temporary copy of the work in the working memory of a computer.”³⁰⁷

To provide counterbalance, however, Article 5(1) of the European Copyright Directive provides an automatic exemption from the reproduction right for “[t]emporary acts of reproduction ... which are transient or incidental, which are an integral and essential part of a technological process whose sole purpose is to enable: (a) a transmission in a network between third parties by an intermediary or (b) a lawful use of a work or other subject-matter to be made, and which have no independent economic significance.” This provision is very similar to the new clause (b) that would have been added to Section 117 of the U.S. copyright statute under S. 1146 and H.R. 3048 (discussed in Section II.A.5(a)(2) above). The Article 5(1) exception would appear to cover the store and forward procedure adopted by routers and the RAM copy produced as a result of browsing at least by a private user (whether browsing for a commercial purpose would have “independent economic significance” is unclear).³⁰⁸ The exception does not apply to computer programs or databases because they are separately regulated in other Directives.³⁰⁹

Thus, the European Copyright Directive adopts an approach that affords the reproduction right a very broad inherent scope, but provides an explicit and automatic exemption for copies that are made incidental to the use³¹⁰ of a work through a technological process, such as transmission through a network or loading into memory for viewing or playing of the work. Indeed, Recital (33) of the European Copyright Directive notes that the exception of Article 5(1) “should include acts which enable browsing as well as acts of caching to take place, including

³⁰⁶ Commentary to Art. 2, ¶ 2.

³⁰⁷ Id. ¶ 3.

³⁰⁸ Justin Harrington & Tina Berking, “Some Controversial Aspects of the EU Copyright Directive (Directive 2001/29/EC),” *Cyberspace Lawyer*, Jan. 2003, at 2, 3-4. The Electronic Commerce Directive contains exemptions in respect of hosting, caching and acting as a mere conduit. Id. at 4.

³⁰⁹ David Schollenberger, “Entertainment Without Borders” (Mar. 2003), at 9 (seminar paper on file with the author).

³¹⁰ An earlier version of Art. 5(1) provided that the use of the work must be “authorized or otherwise permitted by law.” A copy of an earlier version of the European Copyright Directive and comments may be found at www.bna.com/e-law/docs/ecdraft.html (last modified Dec. 2, 1997).

those which enable transmission systems to function efficiently, provided that the intermediary does not modify the information and does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information.”

According to Recital (32) of the European Copyright Directive, the final Directive, unlike its predecessor drafts, opted for an approach of listing “an exhaustive enumeration of exceptions and limitations to the reproduction right and the right of communication to the public.” These exceptions and limitations are enumerated in Articles 5(2) and 5(3). The exceptions and limitations in Article 5(2) apply only to the reproduction right, whereas the exceptions and limitations in Article 5(3) apply to both the reproduction right and the right of communication to the public.

Under Article 5(2), member states may provide for exceptions or limitations to the reproduction right in the following cases:

- (a) in respect of reproductions on paper or any similar medium, effected by the use of any kind of photographic techniques or by some other process having similar effects, with the exception of sheet music, provided that the rightholders receive fair compensation;
- (b) in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly or indirectly commercial, on condition that the rightholders receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work or subject-matter concerned;
- (c) in respect of specific acts of reproduction made by publicly accessible libraries, educational establishments or museums, or by archives, which are not for direct or indirect economic or commercial advantage;
- (d) in respect of ephemeral recordings of works made by broadcasting organizations by means of their own facilities and for their own broadcasts; the preservation of these recordings in official archives may, on the ground of their exceptional documentary character, be permitted;
- (e) in respect of reproductions of broadcasts made by social institutions pursuing non-commercial purposes, such as hospitals or prisons, on condition that the rightholders receive fair compensation.

It is interesting to note that the majority of these exceptions are conditioned upon the rightholders receiving fair compensation, and they cover only copying that is for non-commercial purposes. Exception (b) is of particular interest, for it provides a right for natural persons to make copies for private use and for purposes that are neither directly or indirectly commercial, provided the rightholders receive fair compensation. Presumably the exception would apply where a natural person has purchased a copy of a copyrighted work, thereby providing fair

compensation to the rightholders, and thereafter makes additional copies for personal, noncommercial uses – e.g., by making a copy of one’s purchased music CD onto a cassette for use in one’s car. The drafters of the European Copyright Directive deemed this right of private use to be of such significance that under Article 6(4), member states are permitted to take measures to ensure that beneficiaries of this right are able to take advantage of it, “unless reproduction for private use has already been made possible by rightholders to the extent necessary to benefit from the exception or limitation concerned and in accordance with the provisions of Article 5(2)(b) and (5), without preventing rightholders from adopting adequate measures regarding the number of reproductions in accordance with these provisions.”³¹¹

The right of private use contained in Article 5(2)(b) is similar to a right afforded in the United States under the Audio Home Recording Act (AHRA), 17 U.S.C. § 1008, which provides, “No action may be brought under this title alleging infringement of copyright based on the manufacture, importation, or distribution of a digital audio recording device, a digital audio recording medium, an analog recording device, or an analog recording medium, or based on the noncommercial use by a consumer of such a device or medium for making digital musical recordings or analog musical recordings.” This statute is discussed in detail in Section II.A.7 below, and in Section III.C.2.(c)(1) below in connection with the Napster litigations. Napster, Inc., the operator of a service that enabled subscribers to share music files in MP3 audio format with one another, asserted the AHRA as a defense to an allegation by copyright owners that it was contributorily and vicariously liable for the unauthorized sharing of copyrighted sound recordings through its service. Napster argued that the AHRA permitted its subscribers to share such sound recordings because they were shared for personal use by its subscribers. As discussed in detail below, the courts rejected this argument.

Perhaps in response to online systems like Napster, the drafters of the European Copyright Directive seem to have been concerned that the exception for personal use in Article 5(2)(b) not be construed to permit the unauthorized sharing of copyrighted works in digital form through online systems, at least without compensation to the rightholders affected. Specifically, Recital (38) of the European Copyright Directive states:

Member States should be allowed to provide for an exception or limitation to the reproduction right for certain types of reproduction of audio, visual and audio-visual material for private use, accompanied by fair compensation. This may include the introduction or continuation of remuneration schemes to compensate for the prejudice to rightholders. ... Digital private copying is likely to be more widespread and have a greater economic impact. Due account should therefore be taken of the differences between digital and analogue private copying and a distinction should be made in certain respects between them.

³¹¹ Under the last paragraph of Article 6(4), this right of member states to take measures to ensure that beneficiaries of the right of private use are able to take advantage of it does not apply “to works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them.”

In addition, the drafters of the European Copyright Directive seemed to contemplate that “intermediaries” providing services through which infringing activities take place online should be subject to injunctive relief to stop unauthorized transmissions of copyrighted works through its service. Recital (58) of the European Copyright Directive provides:

In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party’s infringement of a protected work or other subject-matter in a network. This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States.

Under Article 5(3), member states may provide for further exceptions or limitations to the reproduction right and the right of communication to the public in the following cases:

- (a) use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author’s name, is indicated, unless this proves impossible, and to the extent justified by the non-commercial purpose to be achieved;
- (b) uses, for the benefit of people with a disability, which are directly related to the disability and of a non-commercial nature, to the extent required by the specific disability;
- (c) reproduction by the press, communication to the public or making available of published articles on current economic, political or religious topics or of broadcast works or other subject-matter of the same character, in cases where such use is not expressly reserved, and as long the source, including the author’s name, is indicated, or use of works or other subject-matter in connection with the reporting of current events, to the extent justified by the informatory purpose and as long as the source, including the author’s name, is indicated, unless this proves impossible;
- (d) quotations for purposes such as criticism or review, provided that they relate to a work or other subject-matter which has already been lawfully made available to the public, and that, unless this proves impossible, the source, including the author's name, is indicated, and that their use is in accordance with fair practice, and to the extent required by the specific purpose;
- (e) use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings;

- (f) use of political speeches as well as extracts of public lectures or similar works or subject-matter to the extent justified by the informatory purpose and provided that the source, including the author's name, is indicated, except where this proves impossible;
- (g) use during religious celebrations or official celebrations organized by a public authority;
- (h) use of works, such as works of architecture or sculpture, made to be located permanently in public places;
- (i) incidental inclusion of a work or other subject-matter in other material;
- (j) use for the purpose of advertising public exhibition or sale of artistic works, to the extent necessary to promote the event, excluding any other commercial use;
- (k) use for the purpose of caricature, parody or pastiche;
- (l) use in connection with the demonstration or repair of equipment;
- (m) use of an artistic work in the form of a building or a drawing or plan of a building for the purposes of reconstructing the building;
- (n) use by communication or making available, for the purpose of research or private study, to individual members of the public by dedicated terminals on the premises of establishments referred to in paragraph 2(c) of [Article 5(2)] of works and other subject-matter not subject to purchase or licensing terms which are contained in their collections;
- (o) use in certain other cases of minor importance where exceptions or limitations already exist under national law, provided that they only concern analogue uses and do not affect the free circulation of goods and services within the Community, without prejudice to the other exceptions and limitations contained in this Article.

Note that, unlike many of the exceptions of Article 5(2), the exceptions of Article 5(3) are not conditioned upon fair compensation to the rightholders.

6. Peer-to-Peer File Sharing

(a) BMG Music v. Gonzalez

In BMG Music v. Gonzalez,³¹² defendant Cecilia Gonzalez sought to defend her downloading of more than 1370 copyrighted songs through the Kazaa file-sharing network by arguing that her actions should fall under the fair use doctrine on the theory that she was just

³¹² 430 F.3d 999 (7th Cir. 2005).

sampling the music to determine what she liked sufficiently to buy at retail.³¹³ The Seventh Circuit rejected this argument out of hand. Focusing principally on the fourth fair use factor – the effect of the use upon the potential market for or value of the copyrighted work – Judge Easterbrook noted that as file sharing had increased over the last four years, sales of recorded music had dropped by approximately 30%. Although other economic factors may have contributed, he noted that the events were likely related.³¹⁴

He further noted that rights holders had economic interests beyond selling compact discs containing collections of works – specifically, there was also a market in ways to introduce potential consumers to music. Noting that many radio stations stream their content over the Internet, paying a fee for the right to do so, he noted that Gonzalez could have listened to streaming music to sample songs for purchase, and had she done so, the rights holders would have received royalties from the broadcasters.³¹⁵ Rejecting the proffered fair use defense, Judge Easterbrook stated, “Copyright law lets authors make their own decisions about how best to promote their works; copiers such as Gonzalez cannot ask courts (and juries) to second-guess the market and call wholesale copying ‘fair use’ if they think that authors err in understanding their own economic interests or that Congress erred in granting authors the rights in the copyright statute.”³¹⁶

The plaintiffs sought statutory damages for Gonzalez’ unauthorized copying, seeking the minimum amount of \$750 per work infringed. Gonzalez sought to reduce the award below the \$750 minimum by arguing under Section 504(c)(2) that she was not aware and had no reason to believe that her acts constituted infringement of copyright. The district court rejected the request under the provisions of Section 402(d), which provides that if a valid notice of copyright appears on the phonorecords to which a defendant had access, then no weight shall be given to the defendant’s interposition of a defense based on innocent infringement in mitigation of actual or statutory damages.³¹⁷ Gonzalez sought to avoid Section 402(d) by arguing that there were no copyright notices on the data she downloaded. The court rejected this argument: “She downloaded data rather than discs, and the data lacked copyright notices, but the statutory question is whether ‘access’ to legitimate works was available rather than whether infringers earlier in the chain attached copyright notices to the pirated works. Gonzalez readily could have learned, had she inquired, that the music was under copyright.”³¹⁸

³¹³ Id. at 889-90.

³¹⁴ Id. at 890.

³¹⁵ Id. at 891.

³¹⁶ Id.

³¹⁷ Id. at 891-92.

³¹⁸ Id. at 892. Gonzalez also challenged the district court’s award of the \$750 amount on summary judgment, arguing that the choice of amount is a question for the jury. The Seventh Circuit noted that, although a suit for statutory damages under Section 504(c) is a suit at law to which the seventh amendment applies, this does not mean that a jury must resolve every dispute. When there are no disputes of material fact, a court may enter

(b) Columbia Pictures v. Bunnell

In Columbia Pictures Industries, Inc. v. Bunnell,³¹⁹ the court entered judgment against defendant Valence Media LLC, operator of the web site at www.torrentspy.com, for willful inducement of copyright infringement, contributory copyright infringement, and vicarious copyright infringement. The court awarded the plaintiffs statutory damages of \$30,000 per infringement for each of 3,699 infringements shown, for a total judgment of \$110,970,000. The court also issued a permanent injunction enjoining the defendants from encouraging, inducing, or knowingly contributing to the reproduction, download, distribution, upload, or public performance or display of any copyrighted work at issue, and from making available for reproduction, download, distribution, upload, or public performance or display any such work.³²⁰

(c) Sony BMG Music Entertainment v. Tenenbaum

In Sony BMG Music Entertainment v. Tenenbaum,³²¹ the court rejected a broadside fair use defense for the file-sharing by a college sophomore, Joel Tenenbaum, of 30 copyrighted songs belonging to the plaintiffs. Describing the defense raised by the defendant's counsel as "truly chaotic,"³²² the court noted that it represented a version of fair use so broad that it would excuse all file sharing for private enjoyment. As the court described counsel's defense, "a defendant just needs to show that he did not make money from the files he downloaded or distributed – i.e., that his use was 'non-commercial' – in order to put his fair use defense before a jury. Beyond that threshold, the matter belongs entirely to the jury, which is entitled to consider any and all factors touching on its innate sense of fairness – nothing more and nothing less."³²³

The court first turned to the threshold issue of whether fair use is an equitable defense. Noting that a number of courts had suggested that it is, the court nevertheless opined that even if fair use is an entirely equitable defense, it is not clear that its determination requires a jury trial, because judges, not juries, traditionally resolve equitable defenses. However, given that two leading copyright historians had suggested that the equitable label may be a misnomer, and because neither party pressed the point, the court assumed that fair use is a jury question, without resolving the question of the equitable origins of the defense. But because fair use is ultimately a legal question, the court noted that, in the face of the plaintiff's motion for summary judgment on the fair use issue, the defendant could put the defense to a jury only if he showed

summary judgment without transgressing the Constitution. The court noted that Gonzalez had argued for the minimum amount of \$750 per song and the plaintiffs had been content with that amount, which the district court then awarded on summary judgment. *Id.*

³¹⁹ 2008 U.S. Dist. LEXIS 63227 (C.D. Cal. July 10, 2008).

³²⁰ *Id.* at *1-3.

³²¹ 672 F. Supp. 2d 217 (D. Mass. 2009), *rev'd*, 660 F.3d 487 (1st Cir. 2011), *cert. denied*, 132 S. Ct. 2431 (2012).

³²² *Id.* at 220.

³²³ *Id.* at 221.

through specific, credible evidence that the facts relevant to that legal analysis were in dispute. The defendant had failed to do so.³²⁴

Turning to an application of the four fair use factors, the court found that the first factor – purpose and character of the use – favored the plaintiffs. The court rejected the defendant’s binary distinction between “commercial” and “non-commercial” uses under the first factor, noting that the purpose and character of a use must be classified along a spectrum that ranges from pure, large-scale profit-seeking to uses that advance important public goals, like those recognized in the statute. The defendant’s file sharing fell somewhere in between. Although the court was not willing to label it “commercial,” as the plaintiffs urged, the court ruled that because the use was not accompanied by any public benefit or transformative purpose, the first factor cut against fair use.³²⁵ The second factor – nature of the copyrighted work – also cut against fair use because musical works command robust copyright protection.³²⁶

The defendant argued that the third factor – portion of the work used – cut against the plaintiffs because he was alleged to have downloaded only individual songs, but not full albums, and it was the albums in which the plaintiffs registered their copyrights, while the individual songs were works made for hire. The court rejected this argument, noting that under existing file sharing case law, individual songs were regularly treated as the relevant unit for evaluating infringement and fair use of musical works.³²⁷

With respect to the fourth factor – effect on the potential market for the work – the defendant argued that his file sharing made little economic difference to the plaintiffs because the songs at issue were immensely popular and therefore widely available on file sharing networks. The court rejected this as an improper framework for the analysis. Rather, one must consider the effect on the market of the sum of activity if thousands of others were engaged in the same conduct. The plaintiffs had provided evidence that the widespread availability of free copies of copyrighted works on the Internet had decreased their sales revenue, and the defendant had offered no affidavits or expert report to disprove or dispute that evidence.³²⁸

The court’s opinion contains a few other interesting observations with respect to the doctrine of fair use as applied to file sharing. First, citing the case of American Geophysical Union v. Texaco Inc.,³²⁹ the court noted that a fair use determination may be affected by the availability or absence of authorized ways to obtain the work in question. The defendant asserted that the emergence of easy-to-use, paid outlets for digital music, such as the iTunes music store, had lagged well behind the advent of file sharing, and this fact should affect the fair

³²⁴ Id. at 223-24.

³²⁵ Id. at 227-29.

³²⁶ Id. at 229.

³²⁷ Id. at 229-30.

³²⁸ Id. at 230-31.

³²⁹ 60 F.3d 913, 931 (2d Cir. 1994).

use analysis. The court responded that, whatever the availability of authorized digital alternatives was when peer-to-peer networks first became widespread in 1999, it was clear that by August 2004 – when the defendant’s file sharing was detected – a commercial market for digital music had fully materialized. In light of that chronology, the unavailability of paid digital music was simply not relevant to the court’s application of the fair use doctrine.³³⁰

Although granting the plaintiffs’ motion for summary judgment on the defendant’s fair use defense, the court concluded with the following two interesting dicta:

– “[T]he Court does not believe the law is so monolithic, or the principles of fair use so narrow that they could not encompass some instances of file sharing copyrighted works. This Court, unlike others that have spoken on the subject, can envision a scenario in which a defendant sued for file sharing could assert a plausible fair use defense – for example, the defendant who ‘deleted the mp3 files after sampling them, or created mp3 files exclusively for space-shifting purposes from audio CDs they had previously purchased.’ (Berkman Center Br. at 36-37, document # 177-3.) The Court can also envision a fair use defense for a defendant who shared files during a period before the law concerning file sharing was clear and paid outlets were readily available. ... A defendant who shared files online during this interregnum, sampling the new technology and its possibilities, but later shifted to paid outlets once the law became clear and authorized sources available, would present a strong case for fair use.”³³¹

– “As this Court has previously noted, it is very, very concerned that there is a deep potential for injustice in the Copyright Act as it is currently written. It urges – no implores – Congress to amend the statute to reflect the realities of file sharing. There is something wrong with a law that routinely threatens teenagers and students with astronomical penalties for an activity whose implications they may not have fully understood. The injury to the copyright holder may be real, and even substantial, but, under the statute, the record companies do not even have to prove actual damage.”³³²

Following a trial, the jury found that Tenenbaum had willfully infringed the plaintiffs’ copyrights and imposed statutory damages of \$22,500 per song, yielding a total award of \$675,000.³³³ In response to the defendant’s motion for a new trial or remitter, the trial court held that an award of that size, given that Tenenbaum reaped no pecuniary reward from the infringement and the infringing acts caused the plaintiffs minimal harm, violated the due process clause of the Constitution as excessive. The court found the award to be far greater than necessary to serve the government’s legitimate interests in compensating copyright owners and deterring infringement and that, in fact, it bore no meaningful relationship to those objectives. Accordingly, the court reduced the jury’s award to one-tenth the amount, or \$2,250 per

³³⁰ Tenenbaum, 672 F. Supp. 2d at 235-36.

³³¹ Id. at 237-38.

³³² Id. at 237.

³³³ Sony BMG Music Entertainment v. Tenenbaum, 721 F. Supp. 2d 85, 87 (D. Mass. 2010), rev’d, 660 F.3d 487, 514 (1st Cir. Sept. 16, 2011), cert. denied, 132 S. Ct. 2431 (2012).

infringed work (three times the statutory minimum), for a total award of \$67,500. The court noted that such amount was still more than the court itself might have awarded in its independent judgment, but the amount was the greatest amount that the Constitution would permit given the facts of the case.³³⁴ The court also reaffirmed its previous ruling rejecting Tenenbaum's fair use defense.³³⁵

On appeal, the First Circuit reversed, finding that the district court erred when it bypassed Tenenbaum's remittitur arguments based on the excessiveness of statutory damages and reached the constitutional due process issue. The court noted that, under established precedent, a trial court's reduction of compensatory damages must, to avoid *Seventh Amendment* error, allow the plaintiff a new trial. Punitive damage awards, by contrast, may be reduced on due process grounds without offering the plaintiff a new trial without running afoul of the *Seventh Amendment*. In bypassing remittitur and the offer of a new trial, the district court had assumed that statutory damage awards should be treated largely as punitive, not compensatory, awards for *Seventh Amendment* purposes.³³⁶ But the First Circuit found that statutory damages have both a compensatory and punitive element, and further noted that the Supreme Court had ruled in the *Feltner* case³³⁷ that the *Seventh Amendment* provides a right to a jury trial on all issues pertinent to an award of copyright statutory damages. Given these important *Seventh Amendment* issues, the First Circuit held that the district court had erred in not ordering remittitur, which would have afforded a number of possible outcomes that could have eliminated the constitutional due process issue altogether, or at the very least materially reshaped it – e.g., by altering the amount of the award at issue or even the evidence on which to evaluate whether a particular award was excessive.³³⁸

The court also rejected the defendant's argument that no statutory damages can be awarded where harm caused by the defendant has not been proved, and that statutory damages cannot be awarded unless reasonably related to actual damages.³³⁹ The court further rejected a number of challenges to the district court's jury instructions, including a challenge to the instruction that willful infringement means that a defendant had knowledge that his actions constituted copyright infringement or acted with reckless disregard for the copyright holder's rights. The First Circuit joined precedent from sister circuits that had unanimously and routinely found that an infringement is willful under Section 504 if it is knowing or in reckless disregard of the copyright holder's rights.³⁴⁰

³³⁴ *Id.* at 89-90.

³³⁵ *Id.* at 98-99.

³³⁶ *Sony BMG Music Entertainment v. Tenenbaum*, 660 F.3d 487, 514 (1st Cir. 2011), *cert. denied*, 132 S. Ct. 2431 (2012).

³³⁷ *Feltner v. Columbia Pictures Television, Inc.*, 523 U.S. 340 (1998).

³³⁸ *Tenenbaum*, 660 F.3d at 511, 514-15.

³³⁹ *Id.* at 502, 506.

³⁴⁰ *Id.* at 507.

Accordingly, the court affirmed the finding of liability against Tenenbaum and the injunctive relief, but vacated the district court's due process damages ruling and reversed the reduction of the jury's statutory damages award. The court reinstated the jury's award of damages and remanded for consideration of the defendant's motion for common law remittitur based on excessiveness. If on remand, the district court allowed any reduction through remittitur, the First Circuit ruled that the plaintiffs must be given the choice of a new trial or acceptance of remittitur.³⁴¹

On remand, the district court ruled there was no basis for common law remittitur of the award because it was not grossly excessive, inordinate, shocking to the conscience of the court, or so high that it would be a denial of justice to permit it to stand. Tenenbaum had personally received multiple warnings from various sources across several years about downloading and distributing copyrighted materials, including the fact that his activities could subject him to liability of up to \$150,000 per infringement. There was thus ample evidence of willfulness on his part and the need for deterrence based on his blatant contempt of warnings and apparent disregard for the consequences of his actions.³⁴² Turning next to the legal principles set forth by the First Circuit for evaluating a due process challenge to the award, the court ruled that under the applicable standard – a statutory damages award comports with due process as long as it cannot be said to be so severe and oppressive as to be wholly disproportioned to the offense of obviously unreasonable – the award must withstand a due process challenge. The court concluded that, given the deference afforded Congress' statutory award determination and the public harms it was designed to address, the particular behavior of Tenenbaum in the case, and the fact that the award was not only within the range for willful infringement but also below the limit for non-willful infringement, it could not be said that its amount was either wholly disproportioned to the offense or obviously unreasonable.³⁴³

On appeal, the First Circuit affirmed that the \$675,000 statutory damages award did not violate due process, finding that the district court had applied the correct standard to judge the constitutionality of the award and reached the correct result for the reasons the district court had given.³⁴⁴

(d) Capitol Records v. Thomas-Rasset

The case of Capitol Records, Inc. v. Thomas-Rasset³⁴⁵ presented a factual situation very similar to that of the Tenenbaum case. Jammie Thomas-Rasset, an individual, was accused by several record companies of copyright infringement for downloading and distributing their

³⁴¹ Id. at 515.

³⁴² Sony BMG Music Entertainment v. Tenenbaum, 2012 U.S. Dist. LEXIS 119243 at *6-10 (D. Mass. Aug. 23, 2012), aff'd, 719 F.3d 67 (1st Cir. 2013).

³⁴³ Id. at *14-18.

³⁴⁴ Sony BMG Music Entertainment v. Tenenbaum, 719 F.3d 67, 70-72 (1st Cir. 2013).

³⁴⁵ 799 F. Supp. 2d 999 (D. Minn. 2011), rev'd, 692 F.3d 899 (8th Cir. 2012), cert. denied, 133 S. Ct. 1584 (2013).

copyrighted sound recordings through the Kazaa peer-to-peer filing sharing application. Three jury trials were conducted, each of which resulted in a finding of willful infringement. The first jury returned a statutory damages award of \$9,250 per song for a total award of \$222,000 based on the defendant's distribution of 24 songs. The court vacated the verdict, however, and granted a new trial based on its conclusion that it had erred in giving a jury instruction which addressed the existence of a "making available" right. The second jury returned a statutory damages award of \$80,000 per song for a total award of \$1,920,000. Upon motion to set aside the award, the court ruled the award was shocking and unjust and remitted the award to \$2,250 per song, or three times the statutory minimum – the same amount as the district judge used in the Tenenbaum case. The plaintiffs then exercised their right to reject remittitur and requested a new trial. The third jury returned a verdict awarding statutory damages in the amount of \$62,500 for each song, for a total award of \$1,500,000.³⁴⁶

The defendant filed a motion to reduce the damages award on the ground that it violated the due process clause of the Constitution because it bore no reasonable relationship to the actual damages caused by the defendant. The court noted that, although in the past it had endeavored to avoid unnecessary adjudication of a constitution issue by relying upon remittitur, based on the plaintiffs' demonstrated refusal to accept a remittitur and the fact that the defendant had not requested remittitur, the court felt it was required to address the constitutionality of the award. Reviewing the relevant legal authority governing the constitutionality of damage awards, the court concluded that, although the due process clause does not require that a statutory damages award be confined or proportioned to the plaintiff's actual loss or damages, the award should bear *some* relation to the actual damages suffered. That was not the case here.³⁴⁷ "In the case of an individual, like Thomas-Rasset, who infringes by using peer-to-peer networks, the potential gain from infringement is access to free music to build a personal library, which could be purchased, at most, for thousands of dollars, not the possibility of hundreds of thousands – or even millions – of dollars in profits."³⁴⁸

Finding a broad legal practice of establishing a treble award as the upper limit permitted in both statutory and common law contexts to address willful or particularly damaging behavior, the court concluded, with citation to the Tenenbaum case, that "in this particular case, involving a first-time willful, consumer infringer who committed illegal song file-sharing for her own personal use, \$2,250 per song [three times the minimum statutory amount], for a total award of \$54,000, is the maximum award consistent with due process."³⁴⁹

After the court issued this ruling in the Thomas-Rasset case, the First Circuit reversed the Tenenbaum case, finding that the district court should not have reached the constitutional issues, but instead should have relied upon the mechanism of remittitur/new trial to address the

³⁴⁶ Id. at 1002-03.

³⁴⁷ Id. at 1003, *1007-08.

³⁴⁸ Id. at 1010.

³⁴⁹ Id. at 1013.

size of the award. However, it should be noted that the procedural posture in which the district court issued its constitutional ruling in the Thomas-Rasset case, in which a previous rejection of remittitur and election of a new trial had taken place and the defendant had not requested remittitur again, was very different from the procedural posture in which the Tenenbaum court issued its ruling, where the court simply went directly to the constitutional issues in response to the defendant's motion for remittitur or a new trial.

The court in the Thomas-Rasset case issued a permanent injunction prohibiting the defendant from infringing the plaintiffs' copyrights, present or future, in any sound recording. The court rejected, however, the plaintiffs request that the court include language in the injunction barring the defendant from "making available" any of the plaintiffs' sound recordings for distribution.³⁵⁰

Plaintiffs argue that, if Thomas-Rasset makes Plaintiffs' copyrighted works available on a peer-to-peer network, she will have completed all of the steps necessary for her to engage in the same illegal distribution of Plaintiffs' works for which she has already been found liable. Because the Court has held that the Copyright Act does not provide a making-available right, it will not enjoin Thomas-Rasset from making the copyrighted sound recordings available to the public.³⁵¹

On appeal, the plaintiffs argued that the Eighth Circuit should reverse the district court's order granting a new trial and reinstate the first jury's award of \$222,000. The plaintiffs also sought a broadened injunction that would forbid Thomas-Rasset from making their copyrighted sound recordings available for distribution. In summary, the Eighth Circuit held that the plaintiffs were entitled to the remedies they sought: damages of \$222,000 and a broadened injunction that prohibited Thomas-Rasset to make available the plaintiffs' sound recordings for distribution. However, because the verdicts returned by the second and third juries were sufficient to justify those remedies, the court found it unnecessary to consider the merits of the district court's order granting a new trial after the first verdict. And although the court acknowledged the importance of the "making available" legal issue to the plaintiff recording companies, the court ruled that they were not entitled to an opinion on an issue of law that was unnecessary for the remedies sought or to a freestanding decision on whether Thomas-Rasset violated the law by making recordings available.³⁵²

On appeal, Thomas-Rasset lodged no objection to reinstatement of the first verdict, subject to arguments about the constitutionality of the size of the damages. She also offered to acquiesce in the entry of an injunction that would forbid her from making available copyrighted works for distribution, which would render moot the issue whether making works available is part of the distribution right of the copyright holder. In response, the Eighth Circuit observed that it reviews judgments, not decisions on issues. The entitlement of the plaintiffs to the

³⁵⁰ Id. at 1016.

³⁵¹ Id.

³⁵² Capitol Records, Inc. v. Thomas-Rasset, 692 F.3d 899, 901-02 (8th Cir. 2012), cert. denied, 133 S. Ct. 1584 (2013).

remedies sought – damages of \$222,000 and an injunction against making copyrighted works available to the public – were the matters in controversy. That the plaintiffs sought these remedies with the objective of securing a ruling on a particular legal issue did not make that legal issue itself the matter in controversy.³⁵³ “Once the requested remedies are ordered, the desire of the companies for an opinion on the meaning of the Copyright Act, or for a statement that Thomas-Rasset violated the law by making works available, is not sufficient to maintain an Article III case or controversy.”³⁵⁴

With respect to the scope of the injunction that should have been issued, the Eighth Circuit noted that the district court’s refusal to enjoin the making available of the recordings was an error of law, even assuming that the district court was correct in concluding that the distribution right does not include a right of making available, because a district court has authority to issue a broad injunction in cases where a proclivity for unlawful conduct has been shown. Here, Thomas-Rasset’s willful infringement and subsequent efforts to conceal her actions showed such a proclivity. Accordingly, the district court erred after the third trial by concluding that the broader injunction requested by the plaintiffs was impermissible as a matter of law. An injunction against making recordings available was lawful and appropriate under the circumstances, even accepting the district court’s interpretation of the Copyright Act. Because Thomas-Rasset was not resisting expanding the injunction to include that relief, the Eighth Circuit directed the district court to modify the judgment to include the requested injunction.³⁵⁵

With respect to the question of damages, the Eighth Circuit ruled that the district court erred in reducing the third jury’s verdict to \$2,250 per work, for a total of \$54,000, on the ground that this amount was the maximum permitted by the Constitution. Under relevant Supreme Court authority, damages awarded pursuant to a statute violate due process only if they are so severe and oppressive as to be wholly disproportioned to the offense and obviously unreasonable, and that was not the case here. The court noted that Congress set a statutory damages range for willful copyright infringement of \$750 to \$150,000 per infringed work, and the \$222,000 sought was toward the lower end of that broad range. And it noted that the Supreme Court has rejected the notion that the constitutional inquiry calls for a comparison of an award of statutory damages to actual damages caused by the violation – because statutory damages are imposed as a punishment for the violation of a public law, Congress may adjust their amount to the public wrong rather than the private injury, just as if the award were going to the state. Accordingly, the Eighth Circuit concluded that the plaintiffs were entitled to the \$222,000 award they sought, and the question whether the district court correctly granted a new trial after the first verdict was moot.³⁵⁶

³⁵³ Id. at 905.

³⁵⁴ Id. at 906.

³⁵⁵ Id. at 906-07.

³⁵⁶ Id. at 906, 907-10.

7. The Immunity of the Audio Home Recording Act (AHRA)

The Audio Home Recording Act of 1992 (AHRA)³⁵⁷ made two major substantive changes to copyright law. First, Subchapter D of the AHRA (Section 1008) immunizes certain noncommercial recording and use of musical recordings in digital or analog form.³⁵⁸ Section 1008 provides:

No action may be brought under this title alleging infringement of copyright³⁵⁹ based on the manufacture, importation, or distribution of a digital audio recording device, a digital audio recording medium, an analog recording device, or an analog recording medium, or based on the noncommercial use by a consumer of such a device or medium for making digital musical recordings or analog musical recordings.

Second, Subchapters B and C (Sections 1002-1007) of the AHRA require (i) that any “digital audio recording device” (DARD) conform to the “Serial Copyright Management System” (SCMS), which allows unlimited first generation copies of an original source, but prohibits second generation copies (i.e., copies of a copy), and (ii) that manufacturers and distributors of digital audio recording devices and digital audio recording media (such as DAT tape and recordable CDs) pay royalties and file various notices and statements to indicate payment of those royalties.³⁶⁰

(a) The Diamond Multimedia Case

The Ninth Circuit’s rulings with respect to the AHRA in Recording Indus. Ass’n of Am. v. Diamond Multimedia Sys.³⁶¹ are discussed in Section III.C.2(c)(1) below in conjunction with the analysis of the Napster cases.

(b) The Napster Cases

For a discussion of the rulings with respect to the AHRA in the Napster cases, see Section III.C.2(c)(1) below.

(c) The Aimster Case

In In re Aimster Copyright Litigation,³⁶² the plaintiffs brought copyright infringement claims against the Aimster peer-to-peer file sharing site and its operators for secondary liability

³⁵⁷ Pub. L. No. 102-563, 106 Stat. 4244 (1992), codified at 17 U.S.C. §§ 1001-1010.

³⁵⁸ *Nimmer* § 8B.01 (2000).

³⁵⁹ The immunity applies with respect to copyrights in both the sound recordings and any musical compositions embodied therein. *Id.* § 8B.07[C][2], at 8B-90.

³⁶⁰ *Id.* §§ 8B.02 & 8B.03 (2000).

³⁶¹ 180 F.3d 1072 (9th Cir. 1999).

³⁶² 252 F. Supp. 2d 634 (N.D. Ill. 2002), aff’d on other grounds, 334 F.3d 643 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004).

for the infringing distribution of the plaintiffs' copyrighted sound recordings. On a motion for a preliminary injunction, the defendants asserted that the plaintiffs had failed to establish that Aimster's users were engaged in direct copyright infringement because the AHRA provided an affirmative defense. The defendants argued that the AHRA shielded them from liability because it was intended to immunize from liability personal use of copyrighted material by protecting all noncommercial copying by consumers of digital and analog musical recordings, relying on the Ninth Circuit's Diamond Multimedia case, discussed in Section III.C.2(c)(1) below.³⁶³

The court rejected the defendants' reliance on the AHRA, distinguishing the Diamond Multimedia case as follows:

The facts of the instant case and Diamond Multimedia are markedly different. The activity at issue in the present case is the copying of MP3 files from one user's hard drive onto the hard drive of another user. The Rio in Diamond Multimedia, by contrast, "merely [made] copies in order to render portable, or 'space shift,' those files that already reside on a user's hard drive." 180 F.3d at 1079. The difference is akin to a[n] owner of a compact disc making a copy of the music onto a tape for that owner's sole use while away from home versus the owner making thousands of copies of the compact disk onto a tape for distribution to all of his friends. Furthermore, Diamond Multimedia had nothing whatsoever to do with whether the MP3 files on the owner's computers themselves infringed copyrights. Rather, the decision was limited solely to the infringement issue regarding the act of shifting files from a computer to a personal device and whether that copying was subject to the particular requirements of the AHRA. In short, Defendant's reliance on Diamond Multimedia is entirely misplaced.³⁶⁴

(d) Atlantic Recording Corp. v. XM Satellite Radio

In Atlantic Recording Corp. v. XM Satellite Radio, Inc.,³⁶⁵ numerous record companies sued XM Satellite Radio for contributory, vicarious and inducement copyright liability based on XM's offering of digital radio broadcast services together with special receivers marketed as "XM + MP3" players that allowed subscribers to record, retain and library individually disaggregated and indexed audio files from XM broadcast performances. The record companies challenged these capabilities as an infringing "digital download delivery service."³⁶⁶

XM offered several services specifically to XM + MP3 player users that were the subject of the plaintiff's challenge. First, while listening to XM programming, an XM + MP3 user could instantly record any song at the touch of a button. To facilitate such recording, the XM + MP3 player maintained a short-term buffered copy of every broadcast song a user listened to. As a

³⁶³ Id. at 648-49.

³⁶⁴ Id. at 649.

³⁶⁵ 2007 U.S. Dist. LEXIS 4290 (S.D.N.Y. Jan. 19, 2007).

³⁶⁶ Id. at *6.

result, a user could record and store in its entirety any broadcast song he or she heard, even if the user started listening to the song after it began to play.³⁶⁷

Second, XM provided XM + MP3 users with playlists from blocks of broadcast programming which had been disaggregated into individual tracks. XM sent users such digital playlists with title and artist information included. The playlists identified all songs broadcast over a particular channel and during a particular period of time. Users could then scroll through a playlist and select which songs to store for future replay, and which to delete. Using this utility, users could hear and store individual songs without actually listening to XM broadcast programming.³⁶⁸

Third, XM provided to users a search function together with “ArtistSelect” and “TuneSelect” utilities that made it easy for a user to find out when a requested song was being broadcast. XM would send the listener immediate notice when his or her chosen artists or songs were played on any XM channel. The user could then immediately switch channels and store the requested track onto his or her XM + MP3 player.³⁶⁹

Fourth, the XM + MP3 players enabled users to store the approximate equivalent of 1,000 songs recorded from XM broadcasts for as long as the user maintained an XM subscription. Accordingly, the court found that these songs were effectively leased to the XM subscriber for as long as he or she maintained status as a subscriber.³⁷⁰

XM brought a motion to dismiss the copyright claims on the ground that it was shielded from infringement actions by Section 1008 of the AHRA because it was acting as a distributor of a digital audio recording device (DARD) immunized by the AHRA. The court first turned to whether the XM + MP3 players constituted a DARD. The plaintiffs argued that they did not, citing the Ninth Circuit’s decision in Recording Industry Ass’n of Am. v. Diamond Multimedia Sys.,³⁷¹ which held that the Diamond Rio device at issue was not a DARD because it could not make copies from a transmission but instead could make copies only from a computer hard drive, which is exempted under Section 1001(5)(B) of the AHRA. The court distinguished the facts of the Diamond case, noting that the XM + MP3 players could receive from transmissions and were capable of copying without an external computer or computer hard drive.³⁷² “Accordingly, at this stage of the proceeding, relying on plain meaning statutory interpretation

³⁶⁷ Id. at *9.

³⁶⁸ Id.

³⁶⁹ Id. at *9-10.

³⁷⁰ Id. at *10-11.

³⁷¹ 180 F.3d 1072 (9th Cir. 1999).

³⁷² XM Satellite, 200 U.S. Dist. LEXIS 4290 at *14 n.4.

and the definition of a DARD contained in Diamond, until proven otherwise by means of discovery, the Court treats the [XM + MP3 players] as DARDs.”³⁷³

The court next turned to whether the AHRA offered XM complete immunity from the plaintiffs’ copyright claims. XM argued that, because it was a distributor of DARDs, it did have such immunity. The court rejected this argument, noting that, while Section 1008 would protect XM from suit for actions based on the distribution of DARDs, such protection would not act as a wholesale, blanket protection for other conduct that XM might be engaged in beyond such distribution. In particular, XM’s acts as a satellite radio broadcaster could form a separate basis for copyright liability. Indeed, the plaintiffs’ complaint made clear that their claims of copyright infringement were based on XM’s acting without authorization as a commercial content delivery provider that delivered permanent digital copies of sound recordings to those devices without permission from the copyright owner.³⁷⁴

More specifically, the plaintiffs alleged that, in providing services specific to users of XM + MP3 players, XM was acting outside the scope of its statutory license for broadcast service under Section 114 of the copyright statute – XM’s only source of permission to use the plaintiffs’ recordings. Such unauthorized acts, according to the plaintiffs, were encroaching directly on their digital download business.³⁷⁵ The court agreed, finding that by broadcasting and storing copyrighted music on DARDs for later recording by the consumer, XM was acting as both a broadcaster and a distributor, but was paying license fees only to be a broadcaster.³⁷⁶

XM argued that its XM + MP3 player was much like a traditional radio/cassette player and should therefore not be viewed as an improper adjunct to broadcasts. The court rejected this analogy, noting that, in the case of traditional radio/cassette players, the only contact between manufacturers of the devices and users occurred at the point of sale. The court found it quite apparent that the use of a radio/cassette player to record songs played over free radio did not threaten the market for copyrighted works as would the use of a recorder which stores songs from private radio broadcasts on a subscription fee basis. The court further noted that, although XM subscribers might put XM + MP3 players to private use, several court decisions had rejected attempts by for profit users to stand in the shoes of their customers making non-profit or noncommercial uses.³⁷⁷

The court therefore denied XM’s motion to dismiss: “The Court finds that because of the unique circumstances of XM being both a broadcaster and a DARD distributor and its access to the copyrighted music results from its license to broadcast only, that the alleged conduct of XM in making that music available for consumers to record well beyond the time when broadcast, in

³⁷³ Id.

³⁷⁴ Id. at *16-18.

³⁷⁵ Id. at *19.

³⁷⁶ Id. at *20.

³⁷⁷ Id. at *21-22.

violation of its broadcast license, is the basis of the Complaint, and being a distributor of a DARD is not. Thus the AHRA, on these facts, provides no protection to XM merely because they are distributors of a DARD.”³⁷⁸

8. Fair Use Cases

(a) Fox News v. TVEyes

The District Court’s Decision

In Fox News Network, LLC v. TVEyes, Inc.,³⁷⁹ the defendant TVEyes operated a media-monitoring service that enabled its subscribers to track when keywords or phrases of interest were uttered on the television or radio. To do this, TVEyes recorded the content of more than 1,400 television and radio stations, twenty-four hours a day, seven days a week. Using closed captions and speech-to-text technology, TVEyes recorded the entire content of television and radio broadcasts and created a searchable database of that content. The database allowed its subscribers, who included the United States Army, the White House, numerous members of the U.S. Congress, and local and state police departments, to track the news coverage of particular events. For example, police departments used TVEyes to track television coverage of public safety messages across different stations and locations, and to adjust outreach efforts accordingly.³⁸⁰

Upon logging into its TVEyes account, a subscriber would be taken to the Watch List Page, which monitored all of the subscriber’s desired keywords and terms, and organized search results by day, tabulating the total number of times the keyword was mentioned by all 1,400 television and radio stations each day over a 32-day period. While on the Watch List Page, a user could also run a “Google News” search, comparing the mentions of the keyword or term on the Internet with the mentions of the keyword or term on the TVEyes database. A subscriber could also create a custom time range to tabulate the number of times a term had been used in a certain time period, and the relative frequency of such use compared to other terms. Subscribers could set up email alerts for specific keywords or terms, and receive responses one to five minutes after the keyword or term was mentioned on any of the 1,400 television and radio stations TVEyes monitored. TVEyes’ responses to subscribers provided a thumbnail image of the show, a snippet of transcript, and a short video clip beginning 14 seconds before the word was used.³⁸¹

When a subscriber on the Watch List Page clicked on the hyperlink showing the number of times the term was mentioned on a particular day, the subscriber was brought to the Results List Page, which displayed each mention of the keyword or term in reverse chronological order.

³⁷⁸ Id. at *23-24.

³⁷⁹ 2014 U.S. Dist. LEXIS 379 (S.D.N.Y. 2014), rev’d, 883 F.3d 169, 176 (2d Cir. 2018).

³⁸⁰ Id. at 383-84.

³⁸¹ Id. at 384.

Each individual result included a portion of transcript highlighting the keyword and a thumbnail image of the particular show that used the term. When the user clicked the thumbnail image of the show, the video clip began to play automatically alongside the transcript on the Transcript Page, beginning 14 seconds before the keyword was mentioned. TVEyes also featured a Power Search tool that allowed users to run ad-hoc keyword search queries; clicking the thumbnail image would bring the user to the clip's corresponding Transcript Page. Subscribers could save, archive, edit, and download to their personal computers an unlimited number of clips generated by their searches. The clips were limited to ten minutes, and a majority of the clips were shorter than two minutes. All subscribers were required to sign a contractual limitation in a User Agreement, limiting use of downloaded clips to internal purposes. TVEyes had recently added a feature that would block a user from trying to play more than 25 minutes of sequential content from a single station. TVEyes enabled subscribers to email a clip from its web site to anyone, whether or not a TVEyes subscriber. When a recipient clicked on the hyperlink, the viewer was directed to TVEyes' web site, not to the content owner's web site, and could watch the video content in high definition.³⁸²

Fox News brought an action for copyright infringement to enjoin TVEyes from copying and distributing clips of Fox News programs and for damages. TVEyes asserted that its use of Fox News material constituted fair use, and both parties moved for summary judgment. The court ruled that TVEyes' use of Fox News' content was fair use, with exceptions noted with respect to certain questions of fact, and denied Fox News' request for an injunction.³⁸³

The court found that the first fair use factor (purpose and character of the use) favored TVEyes because its service was transformative. The indexing and collecting of visual and audio images provided by the service allowed subscribers to categorize, not only content in response to key search words, but also information that might be just as valuable to subscribers as the content, since a speaker's demeanor, tone, and cadence could often elucidate his or her true beliefs far beyond what a stale transcript or summary could show. Unlike the indexing and excerpting of news articles, where the printed word conveys the same meaning no matter the forum or medium in which it is viewed, the TVEyes service was transformative because it enabled its subscribers to gain access not only to the news that was presented, but to the presentations themselves, as colored, processed, and criticized by commentators, and as abridged, modified, and enlarged by news broadcasts. TVEyes had created a database of otherwise unavailable content – it was the only service that created a database of everything that television channels broadcast, twenty-four hours a day, seven days a week – and made that content searchable.³⁸⁴

The court found the second factor (nature of the copyrighted work) weighed neither for nor against fair use because, where (as here) the creative aspect of the works copied is transformed, the second factor has limited value. The third factor (amount and substantiality of

³⁸² Id. at 384-85.

³⁸³ Id. at 383.

³⁸⁴ Id. at 392-93.

the portion used in relation to the whole) also weighed neither for nor against fair use. The court noted that, where copying the entire work is necessary to accomplish the transformative function or purpose, as was the case here, the third factor must bow to the importance and priority of the first factor's finding of transformative use. Finally, the court found that the fourth factor (economic harm to the value of the work) did not weigh against a finding of fair use in view of the de minimis nature of any possible competition to Fox News when compared to the substantial public service that TVEyes provided. The court found that the facts did not support Fox News' speculation that TVEyes' users actually used TVEyes as a substitute for Fox News' channels in view of the fact that TVEyes erased content every 32 days and in a typical month, fewer than 1% of TVEyes' users played a video clip that resulted from a keyword search of its watch terms and the average play time for a video clip was 41 seconds. The court also rejected Fox News' argument that TVEyes impaired the derivative market for video clips of copyrighted content with syndication partners like YouTube and with Fox News' exclusive licensing agents. Fox News was unable to provide the identity of any customers lost by its partners or licensing agents. The court also noted that Fox News' entire revenue from the derivative sources, between July 1, 2012 and June 30, 2012, was \$459,290, a very small fraction of its overall revenue. Thus, any small market harm to Fox News that might occur was outweighed by the public benefit arising from the TVEyes service.³⁸⁵

Accordingly, the court found that TVEyes' copying of Fox News' broadcast content for indexing and clipping services to its subscribers constituted fair use. However, the court noted that it was not deciding the issue of fair use for the full extent of TVEyes' service. In particular, the parties had not provided sufficient evidence showing that the service's capability to allow subscribers to save, archive, download, email and share clips of Fox News' television programs was integral to the transformative purpose of indexing and providing clips and snippets of transcript to subscribers. Similarly, neither party was entitled to summary judgment on the issue of whether the date and time search function, allowing subscribers to search for television clips by date and time instead of by keyword or term, was integral to the transformative purpose of TVEyes and its defense of fair use. The factual record therefore needed to be developed further before the court could decide whether those uses constituted fair use.³⁸⁶

In a subsequent opinion, the court made rulings with respect to the following features of TVEyes' service:

- Archiving: The ability to archive video clips was integral to the service. Requiring users to go through repeated searches every time they wanted to view previously identified clips would place needless obstacles in the path of prospective researchers, critics, and commentators, and would sharply curtail the value of the service. And longer term, longitudinal studies of the media's treatment of particular subjects would be impossible

³⁸⁵ Id. at 394-97.

³⁸⁶ Id. at 397-98.

without archiving. Because Fox had not identified any actual or potential market harm from archiving, that function constituted a fair use.³⁸⁷

- Emailing and Sharing: TVEyes permitted its subscribers to share identified video clips with others by sending them a URL link to the video on the TVEyes' server via email. Because the URL was public, recipients did not need to possess TVEyes login credential to access the video. The court found that prohibiting email sharing would prevent TVEyes users from realizing much of the benefit of its transformative service. The court noted, for example, that there are many players in the marketplace of ideas, each with supporting staffs of employees, interns, and independent consultants. Once information is located, parties must be able to transmit that information as part of comment, criticism, and debate, which emailing of URL links allowed. However, there was also substantial potential for abuse. Fair use could not be found unless TVEyes developed necessary protections. Were TVEyes not to prevent indiscriminate sharing, it would risk becoming a substitute for Fox's own web site, thereby depriving Fox of advertising revenue. Because TVEyes bore the burden to show fair use, the court ruled that it must develop protocols to reasonably assure that, when subscribers shared video clips, they did so consistent with Section 107. Until the development of reasonable and adequate protections and a satisfactory showing thereof, TVEyes' emailing function could not be considered fair use.³⁸⁸
- Downloading: When a subscriber identified a clip, he could click a button on the page that downloaded the clip to his computer as a local media file. Downloaded clips contained no identifiers, such as watermarks, and could be shared with and accessed by anyone. There was no digital rights management software that limited access rights. The court ruled that downloading was not sufficiently related to TVEyes' transformative services of searching and indexing and posed undue danger to content owners' copyrights. TVEyes argued that downloading allowed researchers to improve efficiency by organizing related clips into folders, which TVEyes' online Media Center did not allow. But the court found that a limitation in TVEyes' user interface was best remedied by improving the user interface; it did not justify creating a path for infringing the copyrights of others. Accordingly, the downloading function was not integral to TVEyes' transformative purpose and was therefore not a fair use.³⁸⁹
- Date-Time Search: TVEyes allowed a user to enter a desired channel and desired start and end date/time (up to a 10-minute window) and TVEyes produced the corresponding transcript and video clip. TVEyes contended the Date-Time search function was a necessary complement to its keyword search because often a keyword search failed to locate the desired video segment. The court found, however, that the feature was not as

³⁸⁷ Fox News Network v. TVEyes, Inc., 124 F. Supp. 3d 325, 333-34 (S.D.N.Y. 2015).

³⁸⁸ Id. at 334-36.

³⁸⁹ Id. at 336-37.

much a “search” tool as a content delivery tool for users who already knew what they sought. In such cases, TVEyes was not so transformational, since users should be able to procure the desired clip from Fox News or its licensing agents, albeit for a fee. The Date-Time search function therefore duplicated Fox’s existing functionality. The court found Fox’s contention that TVEyes’ Date-Time search was likely to cannibalize Fox’s web site traffic and sales by its licensing agents to be persuasive, and accordingly concluded that the feature was not a fair use.³⁹⁰

In subsequent opinions, the court made rulings with respect to proposed limitations on sharing and email features proposed by the parties in a joint submission, and incorporated those rulings into a permanent injunction and final order that prohibited downloading, Date-Time search and sharing on social media web sites rather than by personally directed emails. The injunction also imposed limitations on the number of recipients of content outside a subscriber’s organization’s email domain, and required authentication of recipient email addresses, clear and conspicuous sender notification, clear and conspicuous recipient notification, the blocking of social media sharing, and other miscellaneous terms.³⁹¹

In November, 2015, DirecTV and TVEyes reached a settlement of their dispute, including an agreement in which DirecTV agreed to drop a new lawsuit accusing TVEyes of violating federal communications laws – a case that TVEyes claimed was merely an end run around the ruling that it was protected by the fair use defense. Under the settlement, TVEyes agreed to an injunction barring it from using DirecTV as a source of content. No financial details of the settlement were disclosed in public filings.³⁹²

The Second Circuit’s Decision

On appeal, the Second Circuit reversed the district court’s holding that the Watch function was a fair use (Fox did not challenge the Search function on appeal). The court ruled that inclusion of the Watch function rendered TVEyes’ package of services unprotected by the fair use doctrine, and that conclusion subsumed and obviated the need for consideration of certain functions that were subsidiary to the Watch function, such as archiving, downloading, and emailing the video clips.³⁹³

The court turned to the applicability of each of the four fair use factors. With respect to the first factor, two of the three panel judges found the Watch function to be at least somewhat

³⁹⁰ Id. at 337.

³⁹¹ See Fox News Network, LLC v. TVEyes, Inc., 2015 U.S. Dist. LEXIS 163301 (S.D.N.Y. Nov. 6, 2015); Fox News Network, LLC v. TVEyes, Inc., 2015 U.S. Dist. LEXIS 163302 (S.D.N.Y. Nov. 6, 2015).

³⁹² Bill Donahue, “DirecTV Settles Fight Against TVEyes,” *Law360* (Nov. 25, 2015), available as of Dec. 1, 2015 at <http://www.law360.com/articles/731529>.

³⁹³ Fox News Network, LLC v. TVEyes, Inc., 883 F.3d 169, 176 (2d Cir. 2018). The Second Circuit denied TVEyes’ petition to rehear the case *en banc*. Bill Donahue, “2nd Circ. Won’t Rehear TVEyes Fair Use Case,” *Law360* (May 15, 2018), available as of May 17, 2018 at <http://www.law360.com/articles/1043784>.

transformative because, much like the television customer in the Supreme Court’s Sony case, TVEyes’ clients could view the Fox programming they wanted at a time and place that was convenient to them, rather than at the time and place of broadcast.³⁹⁴ But the Watch function had only a modest transformative character because, notwithstanding the transformative manner in which it delivered content, it essentially republished that content unaltered from its original form, with no new expression, meaning or message. The clients of TVEyes used Fox’s news broadcasts for the same purpose that authorized Fox viewers used those broadcasts – the purpose of learning the information reported. The first factor therefore favored TVEyes only slightly.³⁹⁵

The court observed that the second factor had rarely played a significant role in the determination of a fair use dispute, and it played no significant role here. The court rejected TVEyes’ argument that, since facts are not copyrightable, the factual nature of Fox’s content militated in favor of a finding of fair use. The court observed that those who report the news undoubtedly create factual works, but it could not seriously be argued that, for that reason, others could freely copy and re-disseminate news reports.³⁹⁶

The court found the third factor clearly favored Fox because TVEyes made available virtually the entirety of the Fox programming that TVEyes’ users wanted to see and hear. TVEyes redistributed Fox’s news programming in ten-minute clips, which – given the brevity of the average news segment on a particular topic – likely provided TVEyes’ users with all of the Fox programming they sought and the entirety of the message conveyed by Fox to authorized viewers of the original.³⁹⁷

Finally, the fourth factor favored Fox because the court found the TVEyes service would undercut Fox’s ability to profit from licensing searchable access to its copyrighted content to third parties. The success of the TVEyes business model demonstrated that deep-pocketed consumers were willing to pay well for a service that allowed them to search for and view selected TV clips, and that such market was worth millions of dollars in the aggregate.

³⁹⁴ Id. at 177-78. Concurring judge Lewis Kaplan did not join the characterization of the Watch function as somewhat transformative. Although he found that characterization by the majority to be dicta because the majority found the other fair use factors to be determinative, he nevertheless expressed the view that he was inclined to reject the idea that enhancing the efficiency or convenience with which copies of copyrighted material are delivered to secondary users, in the context in which the Watch function did so, is transformative. Nor was he persuaded by the majority’s reliance on Sony, since that case was decided before Judge Leval’s article introduced the concept of transformative use or purpose into the copyright lexicon. He observed that no Second Circuit opinion since Sony has said, or even suggested, that Sony stands for the proposition that time-shifting in particular, or efficiency-enhancing delivery technology in general, is transformative. Rather, a 2014 Second Circuit opinion had described Sony as a decision finding a non-transformative use to be a fair use. He expressed the view that he would join that case as well as other Second Circuit cases in declining to construe Sony as offering significant guidance regarding transformative use. Id. at 182, 185-89.

³⁹⁵ Id. at 177-78.

³⁹⁶ Id. at 178.

³⁹⁷ Id. at 179.

Consequently, there was a plausibly exploitable market for such access to TV content, and it was proper to consider whether TVEyes displaced potential Fox revenues when TVEyes allowed its clients to watch Fox's copyrighted content without Fox's permission. The court found that such displacement does occur. Since the ability to redistribute Fox's content in the manner that TVEyes did was clearly of value to TVEyes, it (or a similar service) should be willing to pay Fox for the right to offer the content. By providing Fox's content to TVEyes' clients without payment to Fox, TVEyes was in effect depriving Fox of licensing revenues from TVEyes or similar entities. And Fox itself might wish to exploit the market for such a service rather than license it to others. TVEyes had thus usurped a market that properly belonged to Fox. It was of no moment that TVEyes allegedly approached Fox for a license but was rebuffed – the failure to strike a deal satisfactory to both parties did not give TVEyes the right to copy Fox's copyrighted material without payment.³⁹⁸

The court therefore concluded that the Watch function was not a fair use. Because the district court's injunction was shaped by the erroneous conclusion that the Watch function and some features subsidiary to it were fair use, the Second Circuit remanded to the district court to revise the injunction in accordance with the Second Circuit's opinion. The Second Circuit instructed that the district court should enjoin TVEyes from offering its service with the Watch function. However, because Fox did not dispute TVEyes' right to offer its Search function, Second Circuit noted that the district court's injunction must not bar TVEyes from offering a product that includes the Search function without making impermissible use of any protected audiovisual content.³⁹⁹

In January 2019, Fox and TVEyes announced a settlement in which Fox agreed to a permanent injunction against carrying copyrighted content from Fox News.⁴⁰⁰

B. The Right of Public Performance

Section 106 (4) of the copyright statute grants the owner of copyright in a work the exclusive right to perform the work publicly. The right applies to literary, musical, dramatic, and choreographic works, pantomimes, motion pictures and other audiovisual works. It does not apply to pictorial, graphic, sculptural, and architectural works. It also does not apply to sound recordings, other than with respect to public performances by digital transmission,⁴⁰¹ although a

³⁹⁸ *Id.* at 180.

³⁹⁹ *Id.* at 181-82. The court affirmed the district court's conclusion that TVEyes had committed direct infringement. Its conduct was volitional because it decided what audiovisual content to record, copied that content, and retained it for thirty-two days. And such copying, at least to the extent it was done to enable the Watch function, was an infringement.

⁴⁰⁰ Eriq Gardner, "TVEyes Will No Longer Carry Fox News in Negotiated End to Big Copyright Fight," *The Hollywood Reporter* (Jan. 21, 2019), available as of Jan. 21, 2019 at <https://www.hollywoodreporter.com/thr-esq/tveyes-will-no-longer-carry-fox-news-negotiated-end-big-copyright-fight-1177661>.

⁴⁰¹ The Digital Performance Right in Sound Recordings Act of 1995 created a limited public digital performance right in sound recordings as of February 1, 1996. Pub. L. No. 104-39, 109 Stat. 336 (codified at 17 U.S.C. §§ 106,

public performance of a sound recording may infringe the right of public performance of the underlying musical work that is recorded in the sound recording.

Section 101 provides that to perform a work “publicly” means:

(1) to perform ... it at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered; or

(2) to transmit or otherwise communicate a performance ... of the work to a place specified by clause (1) or to the public, by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times.

Because this definition encompasses transmissions of works, it clearly implicates online activity. However, to fall within the public performance right, there must be a transmission of a *performance* of the work, not merely of the work itself. Thus, for example, transmission of the digitally encoded sounds of a musical work to the hard disk of a recipient computer may infringe the right of distribution of the work (as well as the reproduction right), but not the public performance right, because the work is not being *performed*⁴⁰² at the recipient’s end.

1. Isochronous Versus Asynchronous Transmissions

One of the most hotly debated issues concerning the scope of the public performance right in online contexts is whether, to fall within the copyright owner’s right of public performance, the “performance” must be accomplished by a transmitted signal that is capable of immediate conversion to a performance moment-by-moment in time (referred to as an “isochronous transmission”), or whether it is sufficient that the transmitted signal is sent either faster or slower (overall or moment-by-moment) than the embodied performance (referred to as an “asynchronous transmission”).⁴⁰³

The definition of performing a work publicly in Section 101 of the copyright statute was drafted at a time when “transmissions” were generally isochronous transmissions, as in broadcasting. If this definition is read to require an isochronous transmission, then many acts of downloading of works on the Internet (being asynchronous transmissions), even if followed by

114, 115). Certain transmissions of performances are exempt. The exemptions do not apply, however, to an “interactive” service, which the copyright statute defines as a service “one that enables a member of the public to receive a transmission of a program specially created for the recipient, or on request, a transmission of a particular sound recording, whether or not as part of a program, which is selected by or on behalf of the recipient.” 17 U.S.C. §§ 114(d)(1), 114(j)(7).

⁴⁰² The copyright statute provides that “[t]o ‘perform’ a work means to recite, render, play, dance, or act it, either directly or by means of any device or process or, in the case of a motion picture or other audiovisual work, to show its images in any sequence or to make the sounds accompanying it audible.” 17 U.S.C. § 101.

⁴⁰³ K. Stuckey, *Internet and Online Law* § 6.08[4][b], at 6-59 – 6-60 (2013).

in-home playback, may not fall within the public performance right. Performing rights societies have argued to the contrary.⁴⁰⁴ The issue is particularly significant for musical works because different organizations are often responsible for licensing and collecting royalties for public distribution and public performance of musical works.

Even if an isochronous transmission is required for a public performance, the distinction between isochronous and asynchronous transmissions becomes highly blurred on the Internet. Because the Internet is based on packet switching technology, all transmissions through the Internet are in some sense “asynchronous.” Moreover, through use of buffering in memory or storage of information on magnetic or optical storage, either at the transmitting or the receiving end or both, of all or parts of transmitted data, even an asynchronous transmission can effect a smooth, moment-by-moment performance at the receiving end.

One can argue that the determinative factor of whether a public performance has been accomplished should be judged from the perspective of what the recipient perceives, not the transmission technology used (whether isochronous or asynchronous), especially if the transmitting party controls when and what the recipient sees. For example, the Senate Report accompanying the Digital Performance Right in Sound Recordings Act of 1995 suggests that burst transmissions for prompt playback may constitute public performances:

[I]f a transmission system was designed to allow transmission recipients to hear sound recordings substantially at the time of transmission, but the sound recording was transmitted in a high-speed burst of data and stored in a computer memory for prompt playback (such storage being technically the making of a phonorecord), and the transmission recipient could not retain the phonorecord for playback on subsequent occasions (or for any other purpose), delivering the phonorecord to the transmission recipient would be incidental to the transmission.⁴⁰⁵

2. The Meaning of “Publicly”

Section 106 (4) grants the exclusive right to perform a work “publicly.” Section 101 defines performing a work “publicly” to include performance by transmission to an audience that may receive the transmission at different times, at different places, or both. Thus, the mere fact that recipients may download performances of a work at dispersed times on demand through the Internet does not diminish the “public” nature of such performances. For example, in On Command Video Corp. v. Columbia Pictures Industries, Inc.,⁴⁰⁶ the court held that the public performance right was implicated by a system of video cassette players wired to hotel rooms which was capable of transmitting guest-selected movies to the occupants of one room at a time.

⁴⁰⁴ Id.

⁴⁰⁵ S. Rep. No. 104-128, at 39 (1995), reprinted in 1995 U.S.C.C.A.N. 356, 386.

⁴⁰⁶ 777 F. Supp. 787 (N.D. Cal. 1991).

In sum, the breadth of definition of “public” performances makes a variety of online transmissions of “on demand” information potentially within the public performance right. How contemporaneously the playback of that information must be with the transmission in order for there to be deemed a “performance” under current United States law remains to be seen. The WIPO treaties could render many of these issues largely academic in view of the fact that the current public performance right could become subsumed in the potentially broader right of “communication to the public” or “making available to the public” contained in the WIPO treaties discussed below. However, as discussed further below, the implementation of the WIPO treaties in the DMCA takes a minimalist approach and does not adopt separate rights of “communication to the public” or “making available to the public.” Accordingly, the noted uncertainties with respect to the right of public performance are likely to await further clarification through judicial development.

3. Live Nation Motor Sports v. Davis

In Live Nation Motor Sports, Inc. v. Davis,⁴⁰⁷ the plaintiff promoted and produced motorcycle racing events and streamed webcasts of the events on its web site. Although the facts are unclear from the court’s opinion, the defendant provided links to the plaintiff’s web site that enabled users of the defendant’s web site to view the webcasts from the defendant’s web site. The plaintiff sought a preliminary injunction against the defendant, arguing that the defendant’s links to the plaintiff’s web site constituted an unauthorized display and performance of the plaintiff’s copyrighted broadcasts.⁴⁰⁸

The court granted a preliminary injunction enjoining the defendant from providing Internet links to the plaintiff’s webcasts of its racing events or otherwise displaying or performing the plaintiff’s webcasts.⁴⁰⁹ With almost no analysis, the court ruled that the plaintiff had a likelihood of success on its copyright claim because “the unauthorized ‘link’ to the live webcasts that [the defendant] provides on his website would likely qualify as a copied display or performance of [the plaintiff’s] copyrightable material.”⁴¹⁰ The court found a threat of irreparable harm to the plaintiff because the defendant’s links would cause the plaintiff to lose its ability to sell sponsorships or advertisements on the basis that its website was the exclusive source of the webcasts.⁴¹¹

Although the unclear facts of this case make its reach uncertain, it could potentially imply that any unauthorized link that causes material available on another site to be streamed through an unauthorized site could constitute an infringing public display or performance.

⁴⁰⁷ 2006 U.S. Dist. LEXIS 89552 (N.D. Tex. Dec. 11, 2006).

⁴⁰⁸ Id. at *3-4.

⁴⁰⁹ Id. at *18.

⁴¹⁰ Id. at *12.

⁴¹¹ Id. at *15.

4. United States v. ASCAP

In United States v. ASCAP,⁴¹² the district court ruled that the downloading of a digital music file embodying a particular song does not constitute a public performance of that song. The case arose out of an application that Yahoo, RealNetworks and AOL made to ASCAP for a license to publicly perform the musical works of the ASCAP repertoire by means of their respective Internet services. After the parties were unable to agree on a licensing fee, ASCAP applied to the court for a determination of a reasonable fee. The parties cross-moved for partial summary judgment on the issue of whether downloading a digital music file embodying a song constitutes a public performance of the song.⁴¹³

The court noted that the copyright statute provides that, to “perform” a work means to “recite,” “render,” or “play” it, and the plain meanings of each of those terms require contemporaneous perceptibility. Accordingly, the court concluded that for a song to be “performed,” it must be transmitted in a manner designed for contemporaneous perception. The downloading of a music file is more accurately characterized as a method of reproducing that file, rather than performing it.⁴¹⁴ The court also noted that its interpretation was consistent with the Copyright Office’s position in its 2001 DMCA Section 104 Report to Congress, in which the Copyright Office stated that “we do not endorse the proposition that a digital download constitutes a public performance even when no contemporaneous performance takes place.”⁴¹⁵

On appeal, the Second Circuit affirmed this ruling.⁴¹⁶ The Second Circuit agreed with the district court that the ordinary sense of the words “recite,” “render,” and “play” refer to actions that can be perceived contemporaneously. Downloaded songs are not performed in any perceptible manner during the transfers – the user must take some further action to play the songs after download. Because the electronic download itself involves no recitation, rendering, or playing of the musical work encoded in the digital transmission, the court held that such a download is not a performance of that work.⁴¹⁷

⁴¹² 485 F. Supp. 2d 438 (S.D.N.Y. 2007), aff’d, 627 F.3d 64 (2d Cir. 2010), cert. denied, 181 L.Ed.2d 232 (Oct. 3, 2011).

⁴¹³ Id. at 440-41. The applicants conceded that the streaming of a musical work does constitute a public performance. Id. at 442.

⁴¹⁴ Id. at 443-44. The court also found this interpretation consistent with the holdings of those courts that have addressed downloading of music over the Internet using peer-to-peer file transfer programs. For example, the court cited the holding in Maverick Recording Co. v. Goldshteyn, 2006 U.S. Dist. LEXIS 52422 at *8 (E.D.N.Y. July 31, 2006) (“Downloading and uploading copyrighted files from a peer-to-peer network constitutes, respectively, *reproducing and distributing* copyrighted material in violation of 17 U.S.C. § 106.”) (emphasis added). ASCAP, 2007 U.S. Dist. LEXIS 31910 at *14.

⁴¹⁵ Id. at 444 (quoting U.S. Copyright Office, Digital Millennium Copyright Act Section 104 Report to the United States Congress at xxvii-xxviii (Aug. 29, 2001)).

⁴¹⁶ United States v. ASCAP, 627 F.3d 64 (2d Cir. 2010), cert. denied, 181 L.Ed.2d 232 (Oct. 3, 2011).

⁴¹⁷ Id. at 73.

The Second Circuit rejected ASCAP's argument that all downloads fall under clause (2) of the definition of "perform or display a work 'publicly'" in Section 101⁴¹⁸ because downloads "transmit or otherwise communicate a performance," namely the initial or underlying performance of the copyrighted work, to the public. The Second Circuit cited its 2008 ruling in Cartoon Network (discussed in the next subsection) that, when the statute speaks of transmitting a performance to the public, it refers to the performance created by the act of transmission, not simply to transmitting a recording of a performance. ASCAP's alternative interpretation was flawed because, in disaggregating the "transmission" from the simultaneous "performance" and treating the transmission itself as a performance, ASCAP rendered superfluous the subsequent "a performance ... of the work" as the object of the transmittal. Cartoon Network recognized that a "transmittal of a work" is distinct from a transmittal of "a performance" – the former being a transmittal of the underlying work and the latter being a transmittal that is itself a performance of the underlying work. Accordingly, the court ruled that transmittal without a performance does not constitute a "public performance."⁴¹⁹

5. The Cablevision Case

In The Cartoon Network LP v. CSC Holdings, Inc.⁴²⁰ the Second Circuit ruled on whether the playback through Cablevision's network of copies of cable programs stored on its servers at the instance of its customers as part of its "Remote Storage" Digital Video Recorder (RS-DVR) system constituted unauthorized public performances of the stored works. The detailed facts of how the RS-DVR system worked are set forth in Section II.A.4(n) above. Cablevision argued that the transmissions generated in response to customer requests for playback of programs stored on its network servers by customers did not constitute public performances because the RS-DVR customer, not Cablevision, invoked the transmitting and thus the performing, and the transmissions were not "to the public."⁴²¹

The court ruled that it need not address Cablevision's first argument because, even if the court were to assume that Cablevision made the transmissions when RS-DVR playbacks occurred, the RS-DVR playbacks did not involve the transmission of a performance "to the public." The court began its analysis by noting that the second, or "transmit," clause of the definition of public performance applies "whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times."⁴²² The court observed, "The fact that the statute says 'capable

⁴¹⁸ That clause provides that to "perform or display a work 'publicly' means "(2) to transmit or otherwise communicate a performance or display of the work to a place specified by clause (1) or to the public, by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times." 17 U.S.C. § 101.

⁴¹⁹ ASCAP, 627 F.3d at 73-74.

⁴²⁰ 536 F.3d 121(2d Cir. 2008), cert. denied sub nom. CNN, Inc. v. CSC Holdings, Inc., 557 U.S. 946 (2009).

⁴²¹ Id. at 134.

⁴²² Id.

of receiving the performance,’ instead of ‘capable of receiving the transmission,’ underscores the fact that a transmission of a performance is itself a performance.”⁴²³

The Second Circuit therefore focused on who was “capable of receiving” performances through playbacks via the RS-DVR system. Cablevision argued that, because each RS-DVR transmission was made using a single unique copy of a work, made by an individual subscriber, one that could be decoded exclusively by that subscriber’s cable box, only one subscriber was capable of receiving any given RS-DVR transmission. By contrast, the district court had suggested that, in considering whether a transmission was “to the public,” one should consider not the potential audience of a particular transmission, but the potential audience of the underlying *work* whose content was being transmitted. The Second Circuit ruled that the district court’s approach was inconsistent with the language of the transmit clause, which speaks of persons capable of receiving a particular “transmission” or “performance,” and not of the potential audience of a particular “work.”⁴²⁴

On appeal, the plaintiffs presented a slightly different argument, insisting that the same original performance of a work was being transmitted to Cablevision’s various subscribers at different times upon request. The court noted that the implication of the plaintiffs’ argument was that, to determine whether a given transmission of a performance was to the public, one should consider not only the potential audience of that transmission, but also the potential audience of any transmission of the same underlying “original” performance. The court rejected this argument, noting that it would obviate any possibility of a purely private transmission.⁴²⁵

We do not believe Congress intended such odd results. Although the transmit clause is not a model of clarity, we believe that when Congress speaks of transmitting a performance to the public, it refers to the performance created by the act of transmission. Thus, HBO transmits its own performance of a work when it transmits to Cablevision, and Cablevision transmits its own performance of the same work when it retransmits the feed from HBO.⁴²⁶

Accordingly, the Second Circuit concluded that a court must look downstream, rather than upstream or laterally, to determine whether any link in a chain of transmissions made by a party constitutes a public performance, and should not examine the potential recipients of the content provider’s initial transmission to determine who was capable of receiving the RS-DVR playback transmission. Because the RS-DVR system, as designed, made transmissions only to one subscriber using a copy made by that particular subscriber, the court concluded that the universe of people capable of receiving an RS-DVR transmission was the single subscriber whose self-made copy was used to create the transmission, and the transmissions through the RS-

⁴²³ Id.

⁴²⁴ Id. at 135.

⁴²⁵ Id. at 135-36.

⁴²⁶ Id. at 136.

DVR system were therefore not public performances.⁴²⁷ The court cautioned, however, that its holding “does not generally permit content delivery networks to avoid all copyright liability by making copies of each item of content and associating one unique copy with each subscriber to the network, or by giving their subscribers the capacity to make their own individual copies. We do not address whether such a network operator would be able to escape any other form of copyright liability, such as liability for unauthorized reproductions or liability for contributory infringement.”⁴²⁸

6. Ringtones – In re Application of Cellco Partnership

In In re Application of Cellco Partnership d/b/a Verizon Wireless,⁴²⁹ the court ruled that the sale of ringtones by Verizon to its cell phone customers did not require payment to ASCAP for a public performance license for the musical works embodied in the ringtones. ASCAP argued that Verizon engaged in public performances of the musical works when it downloaded ringtones to its customers. It also argued that Verizon was both directly and secondarily liable for public performances of musical works when its customers played ringtones on their telephones upon incoming calls.⁴³⁰

The court rejected both these arguments. As to the first, citing the Cablevision case discussed in the previous subsection, the court ruled that, because only one subscriber was capable of receiving a particular transmission of a ringtone during download, such transmission was not itself made to the “public,” regardless of whether a download could be considered a transmission of a “performance” of the musical works in the ringtone.⁴³¹ The court did note that, “[w]here a transmission is of a digital file rather than a performance that can be contemporaneously observed or heard, and where that transmission is but a link in a chain to a downstream public performance, it may be that the transmission is not an act of infringement for which the transmitter is directly liable under § 106(4), but rather an act that may subject the transmitter to contributory liability under § 106(4) for the infringement created by any ultimate public performance.”⁴³² That could not be the case here, however, because the court concluded that there was no qualifying public performance under § 106(4) when the customer used the ringtone upon an incoming call.

⁴²⁷ Id. at 137, 139. “If the owner of a copyright believes he is injured by a particular transmission of a performance of his work, he may be able to seek redress not only for the infringing transmission, but also for the underlying copying that facilitated the transmission. Given this interplay between the various rights in this context, it seems quite consistent with the Act to treat a transmission made using Copy A as distinct from one made using Copy B, just as we would treat a transmission made by Cablevision as distinct from an otherwise identical transmission made by Comcast.” Id. at 138.

⁴²⁸ Id. at 139.

⁴²⁹ 663 F. Supp. 2d 363 (S.D.N.Y. 2009).

⁴³⁰ Id. at 368.

⁴³¹ Id. at 371.

⁴³² Id. at 374 n.14.

Specifically, the court ruled that, when a ringtone plays on a cellular telephone, even when that occurs in public, the user is exempt from copyright liability under Section 110(4) of the copyright statute, which exempts any “performance of a nondramatic literary or musical work otherwise than in a transmission to the public, without any purpose of direct or indirect commercial advantage and without payment of any fee or other compensation for the performance to any of its performers, promoters, or organizers, if [] there is no direct or indirect admission charge.”⁴³³ The court held that on occasions when Verizon customers had activated their ringtones and the telephones rang in the presence of members of the public at a level where it could be heard by others, such playing of the musical works embodied in the ringtones satisfied all of the requirements of the §110(4) exemption: Verizon customers were not playing the ringtones for any commercial advantage, they did not get paid any fee or compensation for those performances, and they did not charge admission. Accordingly, there was no non-exempt public performance by the users of the ringtones to which Verizon could be secondarily liable.⁴³⁴

The court also rejected ASCAP’s argument that Verizon was directly liable for itself engaging in a public performance of copyrighted musical works when ringtones played in public on customers’ cell phones because it controlled the entire series of steps that allowed and triggered the cellular telephone to perform the musical works in public. The court noted that Verizon’s only role in the playing of a ringtone was the sending of a signal to alert a customer’s telephone to an incoming call, and that signal was the same whether the customer had downloaded a ringtone or not, whether she had set the phone to play a ringtone upon receiving a call or not, whether she was in a public setting or not, and whether she had the ringtone volume turned high or low. And it was the caller, not Verizon, who initiated the entire process that led to the playing of the ringtone. Accordingly, Verizon did not engage in activity constituting direct liability, even if the ringing of its customers’ phones in public constituted public performances.⁴³⁵

7. Arista Records v. Myxer

In Arista Records LLC v. Myxer Inc.,⁴³⁶ the defendant Myxer operated a website that enabled registered users to upload recorded music to the site and then, through the use of Myxer’s software, to transcode the music into a format to create and download ringtones. Users could make ringtones they had created available for download to other users. In addition to uploading and downloading ringtones, Myxer users could play portions of any of the sound recordings on Myxer’s site. Users could also select a sound recording on Myxer’s site and share

⁴³³ Id. at 374 (quoting 17 U.S.C. § 110(4)).

⁴³⁴ Id. at 375. Nor, in order to avoid secondary liability, was Verizon obligated to show that each and every customer would be able to meet its burden of proof that its performance of ringtones in public satisfied the § 110(4) exemption. “The law does not impose an insurmountable burden on Verizon to show precisely how each of its customers has actually used her telephone, but only requires it to demonstrate that customers as a group do not exhibit any expectation of profit when they permit the telephones to ring in public.” Id. at 376.

⁴³⁵ Id. at 376-79.

⁴³⁶ 2011 U.S. Dist. LEXIS 109668 (C.D. Cal. Apr. 1, 2011).

it on certain third party websites such as Facebook. Finally, users could select a sound recording on Myxer's site, often a full-length recording, and "Customize It" (using editing tools provided by Myxer) by selecting a desired start and stop point for a ringtone. UMG Records, a competitor in the ringtone market, contended that, by storing copies of UMG's sound recordings on its servers, allowing users to download copies of its sound recordings to users' cell phones, and allowing users to preview its sound recordings on either the Myxer site or on users' cell phones, Myxer was a direct infringer of UMG's reproduction, distribution and digital public performance rights.⁴³⁷

In a footnote, the court noted that Myxer correctly argued that downloading ringtones to one's personal cell phone is not a public performance. Agreeing with the reasoning of the In re Application of Cellco case, the court ruled that the act of downloading and then playing ringtones so as to alert the individual of an incoming call does not violate the exclusive right of public performance because it is not a "public" performance.⁴³⁸

8. Warner Bros. v. WTV Systems

In Warner Bros. Entertainment Inc. v. WTV Systems,⁴³⁹ the defendants offered a DVD "rental" service called "Zediva" that allowed customers to view streams from DVDs in DVD players hosted on the defendants' premises. To operate the service, the defendants purchased hundreds of DVD players and installed them in cabinets at a data center they leased in Santa Clara, California. The defendants also purchased copies of the plaintiffs' copyrighted works on DVD and placed those DVDs in their DVD players for selection by their customers. Each DVD remained in its respective DVD player while it was transmitted to the defendants' customers on multiple occasions.⁴⁴⁰

When a customer requested a particular work, the defendants, through their Zediva service, started the play process on a particular DVD player holding the requested work, converted the analog video signal from the DVD player into a digital signal using a video adapter, fed the digital signal into a DVD control server that converted the digital signal to a form suitable for streaming across the Internet, converted the digital signal to a format that could be viewed in the player created by the defendants and used on their web site, transmitted the performance via the Internet to the customer, and provided the customer with a custom viewer necessary to view the video stream. To begin the process, the customer clicked on a virtual button on the defendants' web site. Customers were unable to access all the other features available on a particular DVD, such as deleted and extra scenes, or other special DVD features. The defendants maintained exclusive control of their servers, and the customers had no control whatsoever over

⁴³⁷ Id. at *2, *15-18.

⁴³⁸ Id. at *37 n.16.

⁴³⁹ 824 F. Supp. 2d 1003 (C.D. Cal. 2011).

⁴⁴⁰ Id. at 1006-07.

the various servers that the defendants used to direct traffic among their stacks of DVD players.⁴⁴¹

The defendants described the Zediva service as allowing customers to “rent” a particular DVD and DVD player for 14 days. However, customers did not have access to or control over a specific DVD or DVD player. Instead, the defendants streamed the content of the DVD to a customer for a maximum period of four hours, provided that the customer did not pause it for more than one hour during that time. After four hours of total “rental” time or an hour-long pause, whichever occurred first, the defendants used the DVD player containing the same DVD to transmit the work to a different customer. When the first customer made a request to resume viewing, the transmission might be sent from a different DVD or a different DVD player than the one originally used to transmit in the earlier “rental” period. According to the defendants’ web site, if all of the copies of a particular work were “rented out” when a customer wanted to view the work, the customer could request to be notified, via email, when it became available.⁴⁴²

The plaintiffs claimed that the Zediva service infringed their rights of public performance and sought a preliminary injunction, which the court determined the plaintiffs were entitled to. Turning to whether the streams constituted public performances, the court noted that the definition of “public performance” in Section 106(4) is comprised of two clauses: (1) the “public place” clause, which states that a performance is public if it occurs at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered; and (2) the “transmit” clause, which states that a performance is public if someone transmits or otherwise communicates the performance to a place specified by the public place clause, or to “the public,” whether the members of the public capable of receiving the performance receive it in the same place or in separate places and at the same time or at different times.⁴⁴³

The defendants argued that their service offered “DVD rentals” rather than transmissions of performances. The court rejected this argument, analogizing to On Command Video Corp. v. Columbia Pictures Industries,⁴⁴⁴ which held that transmissions of movies from a central console of VCRs (each VCR containing a copy of a particular movie) in a hotel to private guest rooms did not constitute “electronic rentals” similar to guests’ physical borrowing of videotapes, but rather constituted transmissions of performances under the transmit clause of Section 106(4). In On Command, the fact that hotel guests initiated the transmission by turning on the television and choosing a video was immaterial. The court ruled that, as in On Command, the Zediva service fell under the transmit clause because it transmitted performances by communicating the images and sounds of the movies through the use of a device or process (the defendants’

⁴⁴¹ Id. at 1007 & n.2.

⁴⁴² Id. at 1007.

⁴⁴³ Id. at 1008-09.

⁴⁴⁴ 777 F. Supp. 787, 789-90 (N.D. Cal. 1991).

equipment, servers and the Internet) from its central bank of DVD players to individual customer's computers, where the images and sounds were received beyond the place from which they were sent. And as in On Command, the fact that Zediva's customers initiated the transmission by turning on their computers and choosing which of the works they wished to view was immaterial to the legal analysis.⁴⁴⁵

The court further ruled that the transmissions of the Zediva service were "to the public" for purposes of the transmit clause "because the relationship between Defendants, as the transmitter of the performance, and the audience, which in this case consists of their customers, is a commercial, 'public' relationship regardless of where the viewing takes place. The non-public nature of the place of the performance has no bearing on whether or not those who enjoy the performance constitute 'the public' under the transmit clause."⁴⁴⁶

The court rejected the defendants' argument that their performances were not "to the public" in view of the Cartoon Network (Cablevision) case discussed in Section II.B.5 above. Under Cartoon Network, the Second Circuit found that the transmissions were not "to the public" because each RS-DVR playback transmission was made to a single subscriber using a single unique copy produced by that subscriber. By contrast, in this case, the defendants' customers did not produce their own unique copy of the plaintiffs' copyrighted works. Instead, like On Command, the same DVD was used over and over again to transmit performance of the works, which destroyed the one-to-one relationship on which the Cartoon Network decision depended for its finding that the transmissions were not to the public.⁴⁴⁷

The court also rejected the defendants' argument that it should adopt the Second Circuit's volitional requirement for direct copyright infringement liability. The court found that no Ninth Circuit case had adopted the volitional conduct requirement and that, in view of the fact that copyright infringement is a strict liability offense, the court was not inclined to adopt the volitional conduct requirement without clear instruction from the Ninth Circuit.⁴⁴⁸ Finally, the court rejected the defendants' reliance on Professional Real Estate Investors, Inc.,⁴⁴⁹ which involved a service provided by a hotel that rented videodiscs to its guests, who carried the discs to their rooms to watch them on in-room videodisc players. The Ninth Circuit found that because the performances at issue took place in a guest's private hotel room, the performances were not "in public," and the performances were not transmissions under the transmit clause because the guests carried the discs to their rooms, rather than the hotel transmitting a performance to the room from a central bank of players. The Ninth Circuit stated, however, that a closed circuit system similar to the one described in On Command would fall squarely within

⁴⁴⁵ WTV Systems, 824 F. Supp. 2d at 1009-10.

⁴⁴⁶ Id. at 1010.

⁴⁴⁷ Id. at 1011 n.7.

⁴⁴⁸ Id.

⁴⁴⁹ 866 F.2d 278 (9th Cir. 1989).

the transmit clause. Accordingly, the district court found that the Professional Real Estate case supported the court's finding of infringement.⁴⁵⁰

In concluding that the plaintiffs were entitled to a preliminary injunction, the court noted the following forms of irreparable harm: because the defendants were exploiting the plaintiffs copyrighted works without paying the normal licensing fees, they were depriving the plaintiffs of revenue and jeopardizing the continued existence of the plaintiffs' licensees' businesses; the Zediva service threatened the development of a successful and lawful video-on-demand market and, in particular, the growing Internet-based video-on-demand market; the presence of the Zediva service in the market threatened to confuse consumers about video-on-demand products, and to create incorrect but lasting impressions with consumers about what constitutes lawful video-on-demand exploitation of copyrighted works; and the Zediva service threatened the development of a successful and lawful video-on-demand market by offering a sub-optimal customer experience (the defendants admitted they had received complaints about the quality of their service and that a lot of times customers would receive a notice that a particular copyrighted work was temporarily "out of stock" because all DVD players containing that particular work were in use).⁴⁵¹

The case settled in October 2011, with Zediva agreeing to pay \$1.8 million to six major movie studios and to cease showing their movies without permission.⁴⁵²

9. Capitol Records v. MP3tunes

For analysis of this case's rulings with respect to infringement of public performance rights against the operator of a music "locker" service, see Section III.C.6(b)(1)(iii).t below.

10. American Broadcasting v. Aereo

The District Court Decision

The widely followed case of American Broadcasting Cos. v. Aereo, Inc.⁴⁵³ applied the logic of the Cablevision case, discussed in detail in Section II.B.5 above, to adjudicate important issues of the scope of the public performance right. The plaintiffs sought a preliminary injunction to stop Aereo from offering a private streaming service that allowed its users to access live copyrighted content over the Internet through various mobile devices such as PCs, laptops, smartphones, and tablet computers. The plaintiffs' motion for a preliminary injunction was limited in scope, challenging only the aspects of Aereo's service that allowed subscribers to view

⁴⁵⁰ WTV Systems, 824 F. Supp. 2d at 1011.

⁴⁵¹ Id. at 1013-14. The court required the defendants to post a bond of \$50,000 as a condition to issuance of the preliminary injunction. Id. at 1015.

⁴⁵² Melissa Lipman, "DVD Streaming Co. Settles Movie Studios' IP Suit For \$2M," *Law360* (Oct. 28, 2011), available as of Aug. 3, 2012 at <http://www.law360.com/articles/281603>.

⁴⁵³ 874 F. Supp. 2d 373 (S.D.N.Y. 2012), aff'd sub nom. WNET v. Aereo, Inc., 712 F.3d 676 (2d Cir. 2013), rev'd sub nom. American Broadcasting Co. v. Aereo, Inc., 134 S. Ct. 2498, 2504 (2014).

the plaintiffs' copyrighted television programs contemporaneously with the over-the-air broadcast of those programs.⁴⁵⁴

Aereo's service worked as follows. A user of Aereo's system, after logging into his account on Aereo's web site, could navigate through a programming guide to select television programs currently being aired or that would be aired at a later time. If the user selected a program that was currently being aired, the user was given two options, "Watch" and "Record." Selecting "Watch" caused Aereo's system to transmit a web page to the user in which the program started after a short delay, allowing the user to view the program "live," i.e., roughly contemporaneous with its over-the-air broadcast. If the user pressed the "Record" button after having begun watching a program using the "Watch" feature, the Aereo system retained the copy that the user had been watching. If "Record" was not selected, the copy was not retained and could not be viewed again later.⁴⁵⁵

Instead of selecting the "Watch" function at the outset, the user could press the "Record" button to schedule a recording of a program that would be broadcast at a later time or that was currently being aired. However, the "Record" feature could also be used, like the "Watch" feature, to view programs live – users could direct Aereo's system to begin a recording and then immediately begin playback of the recording as it was being made.⁴⁵⁶

The technology that implemented the service, which was designed specifically to take advantage of the reasoning of the Cablevision case, consisted of a large bank of individual antennas that could be "assigned" individually to specific users who wanted to watch or record a program. Specifically, when a user clicked on the "Watch" button, the user's web browser sent a request to Aereo's Application Server, which in turn sent a request and certain information about the user and the requested television program to Aereo's Antenna Server. The Antenna Server allocated resources to the user, including an antenna and transcoder, depending on whether the user was a "static" or "dynamic" user, a distinction based on the user's subscription plan with Aereo. Static users had a set of previously selected antennas that had been assigned to them, whereas dynamic users, who were the vast majority of Aereo's subscribers, were randomly assigned an antenna each time they used Aereo's system. No two users were assigned a single antenna at the same time. The data obtained by a particular antenna while allocated to a particular user was not shared with or accessible by any other Aereo user.⁴⁵⁷

Once these resources were allocated, the Antenna Server sent a "tune" request that directed the user's antenna to tune into a particular broadcast frequency band to obtain the desired program. The Antenna Server also sent a request to the Streaming Server that created a unique directory, assigned to the user, for storing the output data received by the antennas and

⁴⁵⁴ Id. at 375.

⁴⁵⁵ Id. at 377.

⁴⁵⁶ Id.

⁴⁵⁷ Id. at 377-78.

processed by the transcoder. Once that directory was created, an electrical signal was sent from the antenna, processed and converted into data packets, and then sent to the transcoder, which encoded it in a form to be transmitted over the Internet. The encoded data was sent to the Streaming Server, where it was saved on a hard disk to a file in the previously created directory and, once saved, was read from that file into a RAM memory buffer that sent the data to the user over the Internet once a sufficient amount of data (at least six or seven seconds of programming) had accumulated. Essentially the same process occurred when the user engaged the “Record” function, the only substantial difference between the “Watch” and “Record” functions being that when a user engaged the “Record” function, the file saved to the hard disk was tagged as permanent and automatically retained, whereas the file saved using the “Watch” function was not automatically retained unless the user clicked “Record” while the show was still open on the user’s web browser.⁴⁵⁸

The plaintiffs moved for a preliminary injunction. The district court noted that the only significant factual dispute for purposes of that motion concerned the operation of Aereo’s antennas. Aereo contended that each of its antennas functioned separately to receive the incoming broadcast signals. The plaintiffs asserted that Aereo’s antennas functioned collectively as a single antenna, because the individual antennas were packed so closely together on a board that they in effect had a shared metallic substructure which appeared to the incoming signals as one continuous piece of metal. After extensive review of the conflicting testimony of the parties’ experts, the court determined that, based on the evidence at that stage of the proceedings, Aereo’s antennas did indeed function independently – a crucial fact for applicability of the Cablevision case to the facts at hand.⁴⁵⁹

The district court then turned to the first element of establishing entitlement to a preliminary injunction – likelihood of success on the merits. Aereo argued that Cablevision applied to its system because, like the RS-DVR system in Cablevision, its system created unique, user-requested copies that were transmitted only to the particular user that created them, and the performances were thus not public. The plaintiffs distinguished Cablevision on its facts, arguing that because Aereo’s subscribers were watching the programs as they were still being broadcast, they were not using the copies Aereo created for time shifting purposes, and those copies therefore did not “break the chain” of the over-the air transmission received by Aereo. Thus, the plaintiffs contended, Aereo was engaged in a public performance that emanated from the original broadcast signal itself, much like a community antenna which simply passes along a broadcast signal the public. Stated differently, the plaintiffs argued that the stored copies of the signals made by Aereo should be viewed as merely facilitating the transmission of a single master copy – in this case, the broadcast signal – rather than as copies from which a distinct transmission was made.⁴⁶⁰

⁴⁵⁸ Id. at 378-79.

⁴⁵⁹ Id. at 379-81.

⁴⁶⁰ Id. at 385.

The court agreed with Aereo's characterization of its system and rejected the plaintiffs' attempts to distinguish Cablevision. With respect to the copies created by Aereo's system, the court found that they were not mere facilitating copies, but rather were no less materially significant to how the system functioned than the copies created in Cablevision's system. First, Aereo's system created a unique copy of each television program for each subscriber who requested to watch that program, saved to a unique directory on Aereo's hard disks assigned to that user. Second, each transmission that Aereo's system ultimately made to a subscriber was from that unique copy. Third, the transmission of the unique copy was made solely to the subscriber who requested it and no other subscriber was capable of accessing that copy. The court held that these factual similarities of Aereo's service to the Cablevision system suggested that Aereo's service fell within the core of what Cablevision held lawful. The court also ruled the fact that Aereo's users could "share" resources like antennas by using them at different times did not affect the analysis, as it remained clear that the copies Aereo's system made were unique for each user and not shared.⁴⁶¹

The court found other similarities to Cablevision as well. An undercurrent in the Second Circuit's reasoning in Cablevision was that the Cablevision system merely allowed subscribers to enjoy a service that could also be accomplished using any standard DVR or VCR. Similarly, Aereo's functionality substantially mirrored that available using devices such as a DVR or a Slingbox,⁴⁶² which allow users to access free, over-the-air broadcast television on mobile Internet devices of their choosing.⁴⁶³ Moreover, the court found that the analysis the Second Circuit undertook in finding that the performance to the user was made from the copies stored in the Cablevision system rather than from, for example, the incoming stream of data, was equally applicable here. Specifically, Cablevision held that a public performance does not occur merely because a number of people are transmitted the same television program. Nor was the Second Circuit willing to accept the argument that, notwithstanding its creation of unique copies, Cablevision was actually transmitting to its users the performance of that work that occurred when the programming service supplying Cablevision's content transmitted that content to Cablevision. In fact, the Second Circuit expressly refused to look back to the received signal to judge whether Cablevision was engaged in a public performance. The district court therefore observed that, given that each antenna in Aereo's system functioned independently, in at least one respect the Aereo system presented a stronger case than Cablevision for attaching significance to the copies made because, unlike Cablevision in which multiple copies were all

⁴⁶¹ Id. at 385-86 & n.7.

⁴⁶² A Slingbox, when connected to a user's television in the home, digitized the received signals, including live broadcast television, and allowed them to be streamed over the Internet to the user's personal mobile devices. Id. at 377. The district court noted, "Plaintiffs do not appear to contend in this litigation that services such as Slingbox are unlawful, instead claiming that they are 'irrelevant' and that Aereo's service is distinguishable because Slingbox consumers themselves set up the Slingbox in their homes." Id.

⁴⁶³ Id. at 386.

created from a single stream of data, each copy made by Aereo's system was created from a separate stream of data.⁴⁶⁴

The district court also rejected the plaintiffs' attempt to distinguish Cablevision on the ground that Cablevision addressed only copies used for time shifting. The court noted that nowhere in Cablevision did the Second Circuit articulate a requirement that the copies be used for time shifting in order to "break the chain" of transmission from the original broadcaster to the end user. Rather, the Second Circuit's analysis of the public performance claim was entirely directed toward explaining why the copies created by the system in Cablevision were significant and resulted in performances to a limited, non-public audience. Nor did anything in Cablevision turn on the times at which individuals received their transmissions.⁴⁶⁵

Finally, the court rejected the plaintiffs' suggestion that Cablevision addressed only transmissions using the same medium as the initial broadcast that were made to the same device and to the same place as the initial transmission. Although points of distinction from Cablevision, the court found no reason to believe that they had any material bearing on who was "capable of receiving" a particular transmission or whether Aereo "breaks the chain" of transmission.⁴⁶⁶

Accordingly, the court concluded that the plaintiffs were unlikely to succeed on the merits of their public performance claim.⁴⁶⁷ The court, however, issued some words of caution about the scope of its decision. First, the court made clear that it did not accept Aereo's position that the creation of any fixed copy from which a transmission is made always defeats a claim for a violation of the public performance right, because such position would eviscerate the transmit clause given the ease of making reproductions before transmitting digital data. Nor did the court need to resolve Aereo's argument that its antennas, standing alone, defeated the plaintiffs' claims that it was engaged in a public performance. Instead, the court merely pointed out that it had found Aereo's use of single antennas to reinforce its conclusion that the copies created by

⁴⁶⁴ Id. at 386-87.

⁴⁶⁵ Id. at 387-90. The court found the plaintiffs' argument that "complete" time shifting should be required to fit within the contours of Cablevision even less persuasive, as the argument was no longer tied to the rationale that time shifting is required to "break the chain" of the original transmission. For example, an Aereo user who began watching a recording of the Academy Awards, initially broadcast at 6:00 p.m., one minute before the program ended at 11:00 p.m. would not have engaged in complete time shifting, although the chain of transmission would certainly have been "broken" across the nearly five hours of recording before viewing commenced. The court found that the plaintiffs had not provided an argument as to why a user who began watching a recording of a program one minute (or five minutes, or ten minutes) before the broadcast ended was part of a public performance but a user who began watching a minute after the program ended was not. Id. at 393-94.

⁴⁶⁶ Id. at 394.

⁴⁶⁷ In view of its conclusion that the plaintiffs had failed to demonstrate they were likely to succeed in establishing that Aereo's system resulted in a public performance, the court found it need not reach the issue of whether Aereo also could escape liability because it was the consumer, not Aereo, who made the transmissions that the plaintiffs complained of. Id. at 396.

Aereo's system were unique and accessible only to a particular user, as they indicated that the copies were created using wholly distinct signal paths. Because the copies were created from a signal received independently by each antenna, in order to find a "master" copy that was arguably being transmitted, the court would have been required, contrary to Cablevision, to look back to the incoming over-the-air signal rather than simply an earlier step in Aereo's process. Aereo's antennas thus reinforced the significance of the copies its system created and aided the court in finding that Aereo did not create mere facilitating copies.⁴⁶⁸

As such, the Court's holding that Plaintiffs have not demonstrated a likelihood of success is limited. There may be cases in which copies are purely facilitory, such as true buffer copies or copies that serve no function whatsoever other than to pass along a clearly identifiable "master" copy from which the transmission is made. These facts, however, are not before the Court today.⁴⁶⁹

Turning to the other elements for a preliminary injunction, the district court found that the plaintiffs had demonstrated they would suffer irreparable harm because Aereo would damage their ability to negotiate with advertisers by siphoning viewers from traditional distribution channels, in which viewership is measured by Nielsen ratings, into Aereo's service which is not measured by Nielsen, artificially lowering those ratings. Similarly, by poaching viewers from cable or other companies that license the plaintiffs' content, Aereo's activities would damage the plaintiffs' ability to negotiate retransmission agreements, as those companies would demand concessions from the plaintiffs to make up for the decrease in viewership. Aereo's service would also harm the plaintiffs' streaming of their content on their own web sites.⁴⁷⁰

With respect to the balance of hardships, the court found that the balance did not tip decidedly in favor of the plaintiffs. The harm to Aereo of a preliminary injunction would be substantial, as it had sufficient capital to continue operations for just six to seven months, after which it would likely shut down absent investment of further capital. An injunction was also likely to cause Aereo to lose employees and damage its ability to attract investors to obtain new capital, and to diminish its competitive advantage in launching a unique and innovative product. Having concluded that Aereo's service was likely lawful, the court ruled that it could not disregard the harms to Aereo that an injunction would cause by assuming its business was founded on infringement.⁴⁷¹

In sum, the district court concluded that because it could not accept the plaintiffs' attempts to distinguish Cablevision, the plaintiffs had not shown a likelihood of success on the merits. And although they had demonstrated they faced irreparable harm, they had not

⁴⁶⁸ Id. at 396.

⁴⁶⁹ Id.

⁴⁷⁰ Id. at 397-99.

⁴⁷¹ Id. at 402-03.

demonstrated that the balance of hardships decidedly tipped in their favor. Accordingly, the court denied the motion for a preliminary injunction.⁴⁷²

The Second Circuit Decision

On appeal, the Second Circuit affirmed.⁴⁷³ The majority opinion began by reviewing the Second Circuit’s interpretation of the transmit clause in Cablevision and noted several key aspects of that interpretation. First, the phrase “capable of receiving the performance” in the transmit clause refers not to the performance of the underlying work being transmitted but rather to the transmission itself, since the transmission of a performance is itself a performance. Second, the transmit clause directs courts to consider the potential audience of only the performance created by the act of transmission. Third, following an interpretation of the transmit clause first advanced by Professor Nimmer, whether a transmission originates from a distinct or shared copy is relevant to the transmit clause because the use of a unique copy may limit the potential audience of a transmission and thus whether that transmission is made to the public.⁴⁷⁴

The court noted that the preceding summary of Cablevision’s interpretation of the transmit clause established “four guideposts that determine the outcome of this appeal”:

First and most important, the Transmit Clause directs courts to consider the potential audience of the individual transmission. ... Second and following from the first, private transmissions – that is those not capable of being received by the public – should not be aggregated. ... Third, there is an exception to this no-aggregation rule when private transmissions are generated from the same copy of the work. In such cases, these private transmissions *should* be aggregated, and if these aggregated transmissions from a single copy enable the public to view that copy, the transmissions are public performances. ... Fourth and finally, “any factor that limits the *potential* audience of a transmission is relevant” to the Transmit Clause analysis.⁴⁷⁵

Applying these guideposts to the present case, the court found the key facts pertaining to application of the transmit clause to be the same as in Cablevision. Specifically, when an Aereo user elected to invoke the Watch or Record features, Aereo’s system created a unique copy of that program on a portion of a hard drive assigned only to that Aereo user. And when an Aereo user chose to watch the recorded program, the transmission sent by Aereo and received by that

⁴⁷² Id. at 404.

⁴⁷³ WNET v. Aereo, Inc., 712 F.3d 676 (2d Cir. 2013), *rev’d sub nom. American Broadcasting Co. v. Aereo, Inc.*, 134 S. Ct. 2498, 2504 (2014). Judge Chin filed a lengthy dissent. The plaintiffs did not appeal the district court’s factual finding that Aereo’s antennas operated independently, which was the only relevant fact on which the parties disagreed. Id. at 680.

⁴⁷⁴ Id. at 687-88.

⁴⁷⁵ Id. at 689 (citations omitted).

user was generated from that unique copy. Thus, just as in Cablevision, the potential audience of each Aereo transmission was the single user who requested that a program be recorded.⁴⁷⁶

The court rejected a number of arguments put forth by the plaintiffs to distinguish Cablevision. First, the plaintiffs noted that in Cablevision the defendant had a license to transmit programming in the first instance when it first aired the programs, and no such license existed here. The court rejected this, noting that Cablevision did not hold that Cablevision's RS-DVR transmissions were licensed public performances, but rather they were not public performances at all, so no license was needed to make them, whether or not a license was required to first air the programs to the public.⁴⁷⁷

Second, the plaintiffs argued that discrete transmissions should be aggregated to determine whether they are public performances. Because Aereo's discrete transmissions enabled members of the public to receive the same performance (i.e., Aereo's retransmission of a program), they were transmissions made to the public. The court noted that this was nothing more than the Cablevision plaintiffs' interpretation of the transmit clause, as it equated Aereo's transmissions with the original broadcast made by the over-the-air network rather than treating Aereo's transmissions as independent performances. That approach had been explicitly rejected by the Cablevision court. The plaintiffs also argued that the Copyright Act requires all of Aereo's discrete transmissions be aggregated and viewed collectively as constituting a public performance. The plaintiffs argued this was not contrary to Cablevision, because Cablevision held only that transmissions of the same performance or work made by different entities should not be aggregated, but discrete transmissions of the same performance or work made by the same entity should be aggregated to determine whether a public performance has occurred. The court rejected this argument because it required a reading of the transmit clause contrary to that adopted by Cablevision by focusing on the potential audience of the performance or work being transmitted, not the potential audience of the particular transmission.⁴⁷⁸

Third, the plaintiffs argued that Cablevision was based on an analogy to a typical VCR, with the RS-DVR simply an upstream version, but Aereo's system was more analogous to a cable television provider. The court responded that, while it was true that the Cablevision court did compare the RS-DVR system to the stand-alone VCR, those comparisons occurred in the section of the opinion discussing Cablevision's potential liability for infringing the plaintiffs' reproduction right. No part of Cablevision's analysis of the public performance right, however, seemed to have been influenced by any analogy to the stand-alone VCR.⁴⁷⁹

Fourth, the plaintiffs argued that Cablevision's RS-DVR copies broke the continuous chain of retransmission to the public in a way that Aereo's copies did not. Specifically, Aereo's copies

⁴⁷⁶ Id. at 690.

⁴⁷⁷ Id.

⁴⁷⁸ Id. at 690-91.

⁴⁷⁹ Id. at 691.

were merely a device by which Aereo enabled its users to watch nearly live TV, while Cablevision's copies, by contrast, could serve only as the source for a transmission of a program after the original transmission, i.e. the live broadcast of the program, had finished. The court rejected this argument for two reasons. First, Aereo's copies did have the legal significance ascribed to the RS-DVR copies in Cablevision because the user exercised the same control over their playback. Such volitional control over how the copy was played made Aereo's hard disk copies unlike the temporary buffer copies generated incident to Internet streaming only after the user had selected the program to watch. Second, the plaintiffs' argument failed to account for Aereo's user-specific antennas. Each user-associated copy of a program created by Aereo's system was generated from a unique antenna assigned only to the user who requested that the copy be made. The feed from that antenna was not used to generate multiple copies of each program for different Aereo users but rather only one copy – the copy that could be watched by the user to whom that antenna was assigned, and only that user.⁴⁸⁰

Finally, the plaintiffs argued that holding that Aereo's transmissions are not public performances would exalt form over substance, because the Aereo system was functionally equivalent to a cable television provider. The court noted that the same was likely true of Cablevision, which created separate user-associated copies of each recorded program for its RS-DVR system instead of using more efficient shared copies because transmissions generated from the latter would likely be found to infringe copyright holders' public performance right. The court acknowledged that perhaps the application of the transmit clause should focus less on the technical details of a particular system and more on its functionality, but the Second Circuit's decision in Cablevision held that technical architecture matters.⁴⁸¹

The majority opinion made one final point with respect to stare decisis, observing that, though presented as efforts to distinguish Cablevision, the plaintiffs' arguments were really ones to overrule Cablevision. After noting that one panel could not overrule a prior decision of another panel, the court went on to observe that stare decisis was particularly warranted here in view of the substantial reliance on Cablevision, pointing to many media and technology companies that had relied on Cablevision as an authoritative interpretation of the transmit clause. One interesting example the court pointed to was cloud media services that allow their users to store music on remote hard drives and stream it to Internet-connected devices, which apparently had been designed to comply with Cablevision.⁴⁸²

Accordingly, the court ruled that Aereo's transmission of unique copies of broadcast television programs created at its users' requests and transmitted while the programs were still

⁴⁸⁰ Id. at 692-93.

⁴⁸¹ Id. at 693-94.

⁴⁸² Id. at 695 & n.19.

airing on broadcast television were not public performances under Cablevision, and affirmed the district court’s denial of a preliminary injunction.⁴⁸³

The Supreme Court Decision

The Supreme Court granted a petition for certiorari and reversed. Writing for a 6-3 majority, Justice Breyer noted that the case required the Court to answer two questions – whether Aereo “performs” the petitioners’ works at all, and if so, whether it does so “publicly.”⁴⁸⁴

Turning to the first question, the Court first reviewed the history that led Congress to amend the copyright statute to bring the activities of community antenna television (CATV) systems (precursors of cable systems) within the scope of the copyright holder’s public performance right. The Court had held in its 1968 decision in Fortnightly that a service provider did not “perform” copyrighted works by placing antennas on hills above cities and using coaxial cables to carry the signals to the home television sets of subscribers because, unlike broadcasters, the service provider did not select the programs to be viewed, but rather simply delivered the programs received to additional viewers.⁴⁸⁵ And it had extended the logic of Fortnightly in its 1974 decision in Teleprompter to conclude that a CATV provider that carried broadcast television programming into subscribers’ homes from hundreds of miles away was still acting more like a viewer than a broadcaster and therefore did not “perform.” The choice of which broadcast stations to retransmit by the CATV provider was not sufficient to make the provider a broadcaster.⁴⁸⁶

In response to these two decisions, Congress amended the copyright statute in 1976 in large part to reject the Court’s holdings in Fortnightly and Teleprompter. The amendments clarified that to “perform” an audiovisual work means to show its images in any sequence or to make the sounds accompanying it audible, and under this definition, the Court noted, *both* the broadcaster and the viewer of a television program “perform,” because they both show the program’s images and make audible the program’s sounds. Congress also added the transmit clause to broaden the definition of public performances to include transmissions of a performance to the public. Accordingly, the transmit clause made clear that an entity that acts like a CATV system itself performs, even if when doing so it simply enhances viewers’ ability to receive broadcast television signals.⁴⁸⁷

The Court found this history to make it clear that Aereo was not simply an equipment provider. Rather, because Aereo’s activities were substantially similar to those of the CATV

⁴⁸³ Id. at 696.

⁴⁸⁴ American Broadcasting Co. v. Aereo, Inc., 134 S. Ct. 2498, 2504 (2014).

⁴⁸⁵ Id. at 2504-05 (citing Fortnightly Corp. v. United Artists Television, Inc., 392 U.S. 390, 498-400 (1968)).

⁴⁸⁶ Aereo, 134 S. Ct. at 2505 (citing Teleprompter Corp. v. Columbia Broadcasting Sys., 415 U.S. 394, 408-10 (1974)).

⁴⁸⁷ Aereo, 134 S. Ct. at 2505-06.

companies that Congress amended the copyright statute to reach, Aereo, and not just its subscribers, “performed” the works transmitted through its system. The Court recognized that a particular difference between Aereo’s system and the CATV systems at issue in Fortnightly and Teleprompter was that the latter systems sent continuous programming to each subscriber’s television set. In contrast, Aereo’s system remained inert until a subscriber indicated a desire to watch a program, and only at that moment, in automatic response to the subscriber’s request, did Aereo’s system active an antenna and begin to transmit the requested program. However, the Court nevertheless concluded that, given Aereo’s “overwhelming likeness” to the cable companies targeted by the 1976 amendments, this sole technological difference between Aereo and traditional cable companies should not make a critical difference.⁴⁸⁸

Drawing an analogy, the Court noted that subscribers in Fortnightly and Teleprompter could select what programs they wished to view by simply turning the knob on their television sets.

[In Aereo’s system], the signals pursue their ordinary course of travel through the universe until today’s “turn of the knob” – a click on a website – activates machinery that intercepts and reroutes them to Aereo’s subscribers over the Internet. But this difference means nothing to the subscriber. It means nothing to the broadcaster. We do not see how this single difference, invisible to subscriber and broadcaster alike, could transform a system that is for all practical purposes a traditional cable system into “a copy shop that provides its patrons with a library card.”⁴⁸⁹

A dissenting opinion, filed by Justice Scalia and joined by Justices Thomas and Alito, strongly objected to the holding that Aereo itself “performed” the petitioners’ works. The dissent argued that the petitioners’ claim for direct infringement was governed by a simple but profoundly important rule – a defendant may be held directly liable only if it has engaged in volitional conduct that violates the copyright statute. The dissent noted that every Court of Appeals to have considered an automated service provider’s direct liability for copyright infringement had adopted the volitional conduct rule, and further noted that, although the Court itself had not opined on the issue, its cases were fully consistent with a volitional conduct requirement. Under the volitional conduct rule, in the dissent’s view, Aereo could not have direct liability. Unlike video-on-demand services, Aereo did not provide a prearranged assortment of movies and television shows. Rather, subscribers were entirely in control of what particular content was transmitted to them.⁴⁹⁰ “In sum, Aereo does not ‘perform’ for the sole and simple reason that it does not make the choice of content. And because Aereo does not

⁴⁸⁸ Id. at 2506-07.

⁴⁸⁹ Id. at 2507 (quoting the dissent’s opinion analogizing Aereo to a copy shop that provides its patrons with a library card).

⁴⁹⁰ Id. at 2512-14 (Justice Scalia, dissenting).

perform, it cannot be held directly liable for infringing the [petitioners'] public-performance right.”⁴⁹¹

The dissent expressed concern that the majority’s “looks like cable TV” rule would greatly disrupt settled jurisprudence that previously applied a straightforward, bright-line test of volitional conduct directed at the copyrighted work. If that test was not outcome determinative in this case, presumably it would not be outcome determinative in other cases involving technological systems acting in automated responses to subscribers’ directives. The dissent also found it unclear what the majority was proposing to replace the bright-line test.⁴⁹² “Perhaps the Court means to adopt (invent, really) a two-tier version of the Copyright Act, one part of which applies to ‘cable companies and their equivalents’ while the other governs everyone else.”⁴⁹³ Nor, in the dissent’s view, had the majority provided any criteria for determining when its cable-TV-lookalike rule would apply.⁴⁹⁴ The dissent therefore concluded, “It will take years, perhaps decades, to determine which automated systems now in existence are governed by the traditional volitional-conduct test and which get the Aereo treatment.”⁴⁹⁵

It is unclear from the majority opinion whether the dissent’s reading of it to reject the volitional conduct rule is correct. The majority opinion does not mention the volitional conduct rule by name at all, nor cite any of the Court of Appeals decisions cited by the dissent that have adopted the rule. Certainly the majority did not apply that rule to dispose of the case, as the dissent would have. However, the majority opinion made the following statement, which seems in substance to leave open the possibility that the volitional conduct rule might apply in other cases of automated systems or functions that do not bear an “overwhelming likeness” to a cable television system: “In other cases involving different kinds of service or technology providers, a user’s involvement in the operation of the provider’s equipment and selection of the content transmitted may well bear on whether the provider performs within the meaning of the Act.”⁴⁹⁶

Turning to the second question to be decided – whether Aereo was performing the petitioners’ copyrighted works “publicly” – the majority concluded that it was. The parties disagreed concerning what performance Aereo transmitted. Petitioners argued that Aereo transmitted a *prior* performance of their works (the original broadcast performance), whereas Aereo argued that the performance it transmitted was the *new* performance created by its act of transmitting. The Court did not resolve this question, assuming *arguendo* that Aereo was correct. Under this assumption, Aereo transmitted a performance whenever its subscribers watched a program. Aereo argued that, because each transmission was to only one subscriber, those transmissions were not to the public. The court rejected this argument, first on policy

⁴⁹¹ *Id.* at 2514.

⁴⁹² *Id.* at 2516.

⁴⁹³ *Id.*

⁴⁹⁴ *Id.*

⁴⁹⁵ *Id.* at 2517.

⁴⁹⁶ *Id.* at 2507 (majority opinion).

grounds, again finding Aereo's system indistinguishable from cable systems, which do perform publicly. Viewed in terms of Congress' regulatory objectives in the 1976 amendments, the Court found that the technological differences in Aereo's system should not matter. Such differences did not render Aereo's commercial objective any different from that of cable companies. Nor did they alter the viewing experience of Aereo's subscribers. And if Aereo were correct, modern cable systems would be able simply to substitute new technologies similar to Aereo and continue their same commercial and consumer-oriented activities free of copyright restrictions.⁴⁹⁷

In addition, focusing on the text of the transmit clause, the Court noted that Aereo's argument relied on the premise that "to transmit ... a performance" means to make a single transmission. But the Court found that the transmit clause suggests that an entity may transmit a performance through multiple, discrete transmissions.⁴⁹⁸ "That is because one can 'transmit' or 'communicate' something through a *set* of actions."⁴⁹⁹ The Court observed that the fact that a singular noun ("a performance") follows the words "to transmit" does not suggest the contrary, because one can sing a song to his family, whether he sings the same song one-on-one or in front of all together. By the same principle, an entity may transmit a performance through one or several transmissions, where the performance is of the same *work*.⁵⁰⁰ Said the Court:

The *Transmit Clause* must permit this interpretation, for it provides that one may transmit a performance to the public "whether the members of the public capable of receiving the performance ... receive it ... at the same time or at different times." §101. Were the words "to transmit ... a performance" limited to a single act of communication, members of the public could not receive the performance "at different times." Therefore, in light of the purpose and text of the Clause, we conclude that when an entity communicates the same contemporaneously perceptible images and sounds to multiple people, it transmits a performance to them regardless of the number of discrete communications it makes.⁵⁰¹

The Court found it not relevant that Aereo transmitted via personal copies of programs, because the statute applies to transmissions "by means of any device or process." The Court observed that whether Aereo transmitted from the same or separate copies, it performed the same work, it showed the same images and made audible the same sounds. The Court therefore concluded that when Aereo streamed the same television program to multiple subscribers, it transmitted a performance to all of them, and those subscribers constituted members of the "public" because they consisted of a large group of people outside of a family and friends.⁵⁰²

⁴⁹⁷ *Id.* at 2508-09.

⁴⁹⁸ *Id.* at 2509.

⁴⁹⁹ *Id.* (emphasis in the original).

⁵⁰⁰ *Id.*

⁵⁰¹ *Id.*

⁵⁰² *Id.* at 2509-10.

Aereo and many of its *amici* express concern that applying the transmit clause to Aereo's conduct would impose copyright liability on other existing or new technologies, such as storage lockers and cloud computing, that Congress could not possibly have wanted to reach. In response, the majority went somewhat out of its way to reassure that its holding was intended to be specific to Aereo's system and would not necessarily reach other technologies, by making the following statements:

-- "[A]n entity that transmits a performance to individuals in their capacities as owners or possessors does not perform to 'the public,' whereas an entity like Aereo that transmits to large numbers of paying subscribers who lack any prior relationship to the works does so perform."⁵⁰³

-- "[T]he history of cable broadcast transmissions that led to the enactment of the *Transmit Clause* informs our conclusion that Aereo 'perform[s],' but it does not determine whether different kinds of providers in different contexts also 'perform.'"⁵⁰⁴

-- "We have said that ['the public'] does not extend to those who act as owners or possessors of the relevant product. And we have not considered whether the public performance right is infringed when the user of a service pays primarily for something other than the transmission of copyrighted works, such as the remote storage of content. See Brief for United States as *Amicus Curiae* 31 (distinguishing cloud-based storage services because they 'offer consumers more numerous and convenient means of playing back copies that the consumers have *already* lawfully acquired' (emphasis in original))."⁵⁰⁵

-- "Finally, the doctrine of 'fair use' can help to prevent inappropriate or inequitable applications of the Clause."⁵⁰⁶

The District Court's Decision on Remand

On remand, the district court ruled that the plaintiffs were entitled to a nationwide preliminary injunction prohibiting Aereo from retransmitting the plaintiffs' copyrighted works at any time while the works were still being broadcast. This was the scope of injunction that the plaintiffs had originally sought and the district court denied. On remand, the plaintiffs sought to broaden the scope of the preliminary injunction to preclude *any* streaming or retransmission of the plaintiffs' works over the Internet, regardless of when those retransmissions occur. The district court rejected this broadened scope, noting that the narrower scope of injunction was the one sought at the time of the original evidentiary hearing held by the court, and both the

⁵⁰³ Id. at 2510.

⁵⁰⁴ Id.

⁵⁰⁵ Id. at 2510-11.

⁵⁰⁶ Id. at 2511.

Second Circuit and the Supreme Court understood the plaintiffs' motion to be limited to that scope when they rendered their respective decisions.⁵⁰⁷

The plaintiffs contended that the Supreme Court's reasoning in its decision made clear that Aereo's retransmission of the plaintiffs' programs to Aereo's subscribers are public performances, regardless of whether the retransmissions are made at the same time or at different times, and a broader scope of injunction was therefore warranted. The court noted that the plaintiffs might have a valid argument that the Supreme Court's reasoning cast doubt on any distinction between near-simultaneous and fully time-shifted retransmission of copyrighted works for the purposes of determining whether Aereo performed publicly. But the Supreme Court had been careful to limit its holding to the case that the plaintiffs decided to put before the courts at the preliminary injunction stage. And the Supreme Court had explicitly noted that, although Aereo's subscribers could instead direct Aereo to stream the program at a later time, that aspect of Aereo's service was not before the Court. Accordingly, the district court held the plaintiffs to their earlier decision, strategic or otherwise, to seek a preliminary injunction limited in scope to retransmission of their copyrighted works while the works were still being broadcast.⁵⁰⁸

The court also rejected Aereo's attempt to narrow the scope of the injunction to a modest delay, such as ten minutes, after the complete airing of the broadcast. Aereo argued, based on some colloquy at the Supreme Court oral argument, that the Supreme Court intended its ruling to be limited to "near-live retransmission," and specifically something less than a ten-minute delay. The district court rejected this argument, ruling that any question of whether time-delayed retransmissions should be enjoined would be addressed upon consideration of a permanent injunction following the close of discovery.⁵⁰⁹

The court also refused Aereo's request to revisit its earlier findings regarding Aereo's harm to the plaintiffs' retransmission consent negotiations and harm caused by the inability of Nielsen to measure Aereo's viewership on the ground that there was no present basis for a finding that the plaintiffs would be irreparably harmed on those two grounds. The court noted that Aereo did not lodge an interlocutory cross-appeal of the court's preliminary irreparable harm findings and so the court concluded that it need not revisit its earlier factual conclusions regarding Aereo's likely damage to the plaintiffs for purposes of entry of the preliminary injunction. In addition, Aereo had not challenged any of the court's other findings of irreparable harm to the plaintiffs based on loss of subscribers due to cord cutting, loss of control over copyrighted content, and damage to relationships with content providers, advertisers, or licensees. Thus, even putting aside the two factual findings that Aereo sought to relitigate, there was still substantial evidence of irreparable harm to the plaintiffs that Aereo did not challenge. Finally, the court noted that its earlier conclusion that the balance of hardships did not tip decidedly in the plaintiffs' favor was driven largely by its conclusion that the plaintiffs were

⁵⁰⁷ American Broadcasting Cos. v. Aereo, Inc., 2014 U.S. Dist. LEXIS 150555 at *33-39 (S.D.N.Y. Oct. 23, 2014).

⁵⁰⁸ Id. at *36-37.

⁵⁰⁹ Id. at *13, *37-38.

unlikely to succeed on the merits. Given the Supreme Court’s ruling, the plaintiffs were now likely to succeed on the merits, and therefore the plaintiffs no longer needed to show that the balance of hardships tipped *decidedly* in their favor. Nor could Aereo claim harm from its inability to continue infringing the plaintiffs’ copyrights.⁵¹⁰

The district court also rejected two additional defenses interposed by Aereo to the preliminary injunction:

The Section 111 Defense. Aereo argued that, in view of the Supreme Court’s rationale for its decision that Aereo performs in ways similar to cable television systems and therefore Congress would have intended the transmit clause to cover Aereo’s activity, Aereo’s system should be considered a “cable system” that is entitled to a compulsory license under Section 111 of the copyright statute. The court rejected Aereo’s argument for a number of reasons. First, the court found that the argument suffered from the fallacy that simply because an entity performs copyrighted works in a way similar to cable systems it must then be deemed a cable system for all other purposes of the Copyright Act. The Supreme Court’s opinion in *Aereo* had not made any such express holding. The district court noted that the Supreme Court had consistently stated throughout its opinion that Aereo’s similarity to a cable system informed its conclusion that Aereo performs, not that Aereo is a cable system. But the Supreme Court did not imply, much less hold, that simply because an entity performs publicly in much the same way as a cable system, it is necessarily a cable system entitled to a Section 111 compulsory license.⁵¹¹ “Stated simply, while all cable systems may perform publicly, not all entities that perform publicly are necessarily cable systems, and nothing in the Supreme Court’s opinion indicates otherwise.”⁵¹²

Aereo argued that such a holding could be inferred from the questions and statements of the Justices at oral argument. The district court rejected this argument, noting that the commentary of individual Justices at oral argument has no legal effect, only the Justices’ written opinions have the force of law.⁵¹³ And the district court observed that any void left by the Supreme Court’s decision on Section 111 was filled by on-point, binding Second Circuit precedent – *WPIX, Inc. v. ivi, Inc.*⁵¹⁴ – which concluded that Congress did not intend for Section 111’s compulsory license to extend to Internet transmissions. In reaching its conclusion, the Second Circuit in *WPIX* had given deference to the Copyright Office’s interpretation that Internet

⁵¹⁰ *Id.* at *30-33.

⁵¹¹ *Id.* at *15-19.

⁵¹² *Id.* at *19.

⁵¹³ *Id.* at *19.

⁵¹⁴ 691 F.3d 275 (2d Cir. 2012), cert. denied, 133 S. Ct. 1585 (2013). The Second Circuit’s decision is discussed in Section III.E.5(a) below.

retransmission services do not constitute cable systems under Section 111, and the district court noted that the Copyright Office had not changed its interpretation of Section 111 since *WPIX*.⁵¹⁵

Aereo contended that the Supreme Court implicitly overruled *WPIX* when it compared Aereo to a cable system. The district court rejected this, noting that the Supreme Court did not mention *WPIX* or its holding, and nothing in the Supreme Court's opinion could be read as abrogating *WPIX*, because the Supreme Court limited its holding to a finding that Aereo performed like a cable system for purposes of the transmit clause, not that it was a cable system entitled to a Section 111 license. The district court therefore concluded that *WPIX* remained good law and binding precedent. The court also rejected Aereo's argument that even if *WPIX* remained good law, the case was distinguishable from the facts here based on the limited geographic reach of Aereo's services – namely, Aereo's technology did not give its subscribers access to broadcasts outside of their home designated market area (DMA). The court noted that the geographic reach of Internet retransmission services was but one of many factors the Second Circuit considered in reaching its holding that Section 111 does not cover Internet retransmission services, and the Second Circuit had referenced the possible geographic reach of *ivi*'s system only as an additional point of distinction between Internet retransmission and traditional cable systems, but it was not the determinative fact for the Second Circuit. Accordingly, the district court ruled that Aereo was not entitled to the Section 111 compulsory license.⁵¹⁶

The Section 512(a) Safe Harbor. Aereo further argued that its “Watch Now” feature fell within the Section 512(a) safe harbor because Aereo was a service provider offering the transmission, routing, or providing of connections for digital online communications. However, Aereo's brief declared only that it qualified as a service provider, but did not explain how it satisfied the statutory definition of that term.⁵¹⁷ The district court noted that the Second Circuit had ruled that to qualify as a service provider for purposes of Section 512(a), an entity must be a mere “conduit.”⁵¹⁸ Aereo was acting as more than a mere conduit by storing and providing links to copyrighted material. Moreover, Aereo had failed to satisfy the provision of Section 512(a)(1) stating that the safe harbor is available only if the transmission of the material was initiated by or at the direction of a person other than the service provider. Here, the Supreme Court had held that Aereo was itself performing the plaintiffs' works, so the transmission of those works was not being initiated solely at the direction of its users. Finally, Aereo had not even alleged that it satisfied the predicate condition of Section 512(i) that it have in place a policy for terminating repeat infringers, and such failure constituted an absolute bar to Aereo being able to assert any defense under Section 512.⁵¹⁹

⁵¹⁵ American Broadcasting Cos. v. Aereo, Inc., 2014 U.S. Dist. LEXIS 150555 at *20-21 & *25 n.3.

⁵¹⁶ Id. at *21-27.

⁵¹⁷ Id. at *27.

⁵¹⁸ Id. at *28 (citing Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 39 (2d Cir. 2012)).

⁵¹⁹ Aereo, 2014 U.S. Dist. LEXIS 150555 at *28-29.

On May 7, 2015, a bankruptcy court in Manhattan approved a settlement granting the plaintiffs a permanent injunction and \$950,000 cash on account of their \$100 million in copyright infringement claims. There was no opposition to the settlement. As part of the bankruptcy proceedings, Aereo engaged in a sale of its assets for a disappointing \$1.65 million.⁵²⁰

11. The BarryDriller Case

The district court in this case reached the opposite result from the district court in the Aereo case on very similar facts involving the defendants' "Aereokiller" streaming service that allowed users to use an individual mini digital antenna and DVR to watch or record a free television broadcast. Indeed, the defendants opposed the plaintiff's motion for a preliminary injunction in this case largely on the argument that their streaming service was legal because it was "technologically analogous" to the service found legal in the Aereo case.⁵²¹ The BarryDriller court, however, rejected the reasoning of the Second Circuit's decision in Cablevision, upon which the Aereo court had relied in reaching its decision. In particular, the court disagreed with the Second Circuit's analysis in Cablevision that the statutory definition of "public performance" requires that a transmission of a performance itself be public in order for the transmitter to infringe the public performance right:

That is not the only possible reading of the statute. The definition section sets forth what constitutes a public performance of a copyrighted *work*, and says that transmitting a performance to the public is a public performance. It does not require a "performance" of a performance. The Second Circuit buttressed its definition with a "cf." to *Buck v. Jewell-La Salle Realty Co.*, 283 U.S. 191, 196, S. Ct. 410, 75 L.Ed. 971 (1931), which interpreted the 1909 Copyright Act's provision of an exclusive right to publicly perform a musical composition and held that "the reception of a radio broadcast and its translation into audible sound" is a performance. But *Buck*, like *Cablevision* and this case, was concerned with a copyright in the work that was broadcast. *Id.* at 195. The Supreme Court was not concerned about the "performance of the performance" – instead, it held that using a radio to perform the copyrighted song infringed the exclusive right to perform the song (not to perform the performance of the song). *Id.* at 196.⁵²²

⁵²⁰ Bill Rochelle, "Broadcasters Get Permanent Injunction Against Aereo Barring Streaming Service," *BNA's Electronic Commerce & Law Report* (May 8, 2015) (ISSN 1523-5661).

⁵²¹ Fox Television Stations, Inc. v. BarryDriller Content Systems, PLC, 2012 U.S. Dist. LEXIS 184209 at * 3-4 (C.D. Cal. Dec. 27, 2012). Before turning to its main analysis, the court rejected in a footnote the plaintiffs' apparent argument that creation of a buffer copy in the course of streaming is itself a public performance: "Plaintiffs seems to be relying on the fact that courts have found 'streaming' to be infringement of the transmission right, and are arguing that streaming's use of buffer copies means that the buffer copy is itself a public performance. But Plaintiffs have cited to no authority that holds that the act of creating the transient buffer copy – expressly considered in *Cablevision* and held not to be an act of infringement – is an infringement of the public performance right. *Cablevision*, 536 F.3d at 127." *Id.* at *12 n.9.

⁵²² *Id.* at *14-15.

The district court noted that the Second Circuit had supported its decision via citation to the House Report on the 1976 Copyright Act, which stated that a performance made available by transmission to the public at large is “public” even though the recipients are not gathered in a single place, and that the same principles apply whenever the potential recipients of the transmission represent a limited segment of the public, such as the occupants of hotel rooms or the subscribers of a cable television service. From this, the Second Circuit reasons that the *transmission* had to itself be public, and one must therefore look at the persons who are capable of receiving a particular transmission of a performance to determine whether such transmission constitutes a public performance.⁵²³ The district court rejected the Second Circuit’s interpretation of the import of the House Report:

But the House Report did not discuss *which copy* of a work a transmission was made from. The statute provides an exclusive right to transmit a performance publicly, but does not by its express terms require that two members of the public receive the performance from the same transmission. The statute provides that the right to transmit is exclusive “whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times. 17 U.S.C. § 101. Again, the concern is with the performance of the copyrighted *work*, irrespective of which copy of the work the transmission is made from. ... Thus, *Cablevision’s* focus on the uniqueness of the individual copy from which a transmission is made is not commanded by the statute.⁵²⁴

The district court noted that the Second Circuit’s focus on which copy of the work the transmission is made from put it in tension with the 1991 decision in the On Command Video Corp. case,⁵²⁵ in which a court in the Northern District of California held that a hotel system that transmitted to individual hotel rooms movies being played from individual videotapes by remote control from a central bank in a hotel equipment room violated the copyright holder’s public performance right. The district court believed that the On Command Video Corp. case properly focused on the public performance of the copyrighted *work*. Accordingly, the court concluded that the defendants’ unique-copy transmission argument based on Cablevision and Aereo was not binding in the Ninth Circuit.⁵²⁶

Having found that the plaintiffs had established a likelihood of success on the merits, and finding the other three factors for a preliminary injunction weighed in the plaintiffs’ favor, the

⁵²³ Id. at *15.

⁵²⁴ Id. at *16. The court elaborated further in a footnote: “The Second Circuit appears to implicitly bracket the text of the House Report like this: [a performance made available by] [transmission to the public]. It seems like the House Report could just as easily be read like this: [a performance made available by transmission] [to the public]. Defendants make Plaintiffs’ copyrighted works available to the public by transmission. The Second Circuit’s reading effectively converts ‘available by transmission’ to ‘available by a single transmission.’ In any event, the *statute* uses the verb ‘transmit,’ rather than the noun used in the House Report.” Id. at *16-17.

⁵²⁵ 777 F. Supp. 787 (N.D. Cal. 1991).

⁵²⁶ BarryDriller, 2012 U.S. Dist. LEXIS at *17-18, 20.

court issued a preliminary injunction against the operation of the Aereokiller service. However, given the court's finding that the application of Ninth Circuit law differed from Second Circuit law, the court believed that principles of comity prevented the entry of an injunction that would apply to the Second Circuit, and that it should not assume that the other Circuits would agree with its decision rather than Cablevision. Accordingly, the court issued an injunction prohibiting the defendants from offering their service only within the states covered by the Ninth Circuit.⁵²⁷

After the district court's decision, the Supreme Court issued its decision in the case of American Broadcasting v. Aereo, discussed in Section II.B.10 above, ruling that Aereo violated the public performance right by transmitting the plaintiffs' works through its system collectively to public subscribers. Given the close factual similarity between the "Aereokiller" service and the Aereo service, the Supreme Court's holding in the Aereo decision would seem to confirm the district court's outcome in this case.

12. Fox v. FilmOn

This was the third case to adjudicate claims of infringement of the public performance right based on a streaming and recording system that operated in a very similar way to those at issue in the Aereo and BarryDriller cases by allowing users to use an individual mini digital antenna and DVR to watch or record a free television broadcast.⁵²⁸ Indeed, FilmOn, the operator of the system, readily admitted that its technology was "similar ... in every relevant way" to the technology at issue in Aereo and BarryDriller.⁵²⁹ The court issued a preliminary injunction enjoining FilmOn from offering its service through the U.S. except within the Second Circuit (where Aereo was the binding precedent), and required the plaintiffs to post a bond of \$250,000.⁵³⁰

To judge the plaintiffs' likelihood of success on the merits of their claim that FilmOn's system infringed their right of public performance, the court pointed to the legislative history of the transmit clause in the House Report for the 1976 Act, which stated, "Under the definitions of 'perform,' 'display,' 'publicly,' and 'transmit' in *section 101*, the concepts of public performance and public display cover not only the initial rendition or showing, but also any further act by which that rendition or showing is transmitted or communicated to the public."⁵³¹ The court noted that the House Report further elaborated on the transmit clause, stating, "Each and every method by which the images or sounds comprising a performance or display are picked up and

⁵²⁷ Id. at 23-29.

⁵²⁸ Fox Television Stations, Inc. v. FilmOn X LLC, 966 F. Supp. 2d 30 (D.D.C. 2013).

⁵²⁹ Id. at 34.

⁵³⁰ Id. at 51-52.

⁵³¹ Id. at 45 (quoting H.R. Rep. No. 94-1476 (1976), *reprinted in* 1976 U.S.C.C.S.A.N. 5659, 5676-77).

conveyed is a ‘transmission,’ and if the transmission reaches the public in [an]y form, the case comes within the scope of *clauses (4) or (5) of section 106.*”⁵³²

In view of the legislative history, the court found that FilmOn’s service violated the plaintiffs’ right of public performance:

By making available Plaintiffs’ copyrighted performances to any member of the public who accesses the FilmOn X service, FilmOn X performs the copyrighted work publicly as defined by the Transmit Clause: FilmOn X “transmit[s] ... a performance ... of the work ... to the public, by means of any device or process.” *See 17 U.S.C. § 101.* “A ‘device,’ ‘machine,’ or ‘process’ is one now known [*i.e.* in 1976] or later developed;” “[t]o ‘transmit’ a performance or display is to communicate it by any *device or process.*” *Id.* (emphasis added). These two definitions are facially broad and encompass FilmOn X’s convoluted process for relaying television signals. The Transmit Clause, which applies whether “members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times,” also plainly captures FilmOn X’s DVR-like capabilities. *Id.* FilmOn X transmits (*i.e.*, communicates from mini-antenna through servers over the Internet to a user) the performance (*i.e.*, an original over-the-air broadcast of a work copyrighted by one of the Plaintiffs) to members of the public (*i.e.*, any person who accesses the FilmOn X service through its website or application) who receive the performance in separate places and at different times (*i.e.* at home at their computers or on their mobile devices).⁵³³

The court rejected FilmOn’s argument that it did not perform publicly because its system facilitated a one-to-one relationship between a single mini antenna and a viewer of the plaintiffs’ programs. The court observed that, while each user might have an assigned antenna and hard-drive directory temporarily, the mini antennas were networked together so that a single tuner server and router, video encoder, and distribution endpoint could communicate with them all. In the court’s view, FilmOn’s system, through which any member of the public could click on the link for the video feed, was hardly akin to an individual user stringing up a television antenna on the roof. The court also expressed the belief that every broadcast of a television program (whether cable, satellite, over-the-air, over the Internet, or otherwise) could be described as generated from the same copy – the original source. The court therefore found FilmOn, a commercial service retransmitting the plaintiffs’ television performances, to be in no meaningful way different from cable television companies, whose relationship with broadcasters was the primary motivation for the 1976 Act’s enactment of the transmit clause.⁵³⁴

⁵³² *Id.* at 45-46 (quoting 1976 U.S.C.C.S.A.N. at 5678).

⁵³³ *Id.* at 46-47. The court noted that it respectfully disagreed with the Second Circuit’s interpretation of the transmit clause in Aereo for the reasons set forth in BarryDriller and in Judge Chin’s dissent in Aereo. *Id.* at 47 n.11.

⁵³⁴ *Id.* at 47-48.

Accordingly, the court concluded that the plaintiffs had established a likelihood of success on the merits of their copyright infringement claim. Finding that the plaintiffs would suffer irreparable harm if FilmOn were allowed to continue operation of its system, that the balance of harm tipped in the plaintiffs' favor, and that the public interest would be served by upholding copyright protection, the court issued a preliminary injunction against FilmOn.⁵³⁵

After the district court's decision, the Supreme Court issued its decision in the case of American Broadcasting v. Aereo, discussed in Section II.B.10 above, ruling that Aereo violated the public performance right by transmitting the plaintiffs' works through its system collectively to public subscribers. Given the close factual similarity between the FilmOn system and the Aereo system, the Supreme Court's holding in the Aereo decision would seem to confirm the district court's outcome in this case, and in a subsequent ruling the district court concluded that it did.

Specifically, in later proceedings, the defendants argued that under the rationale of the Supreme Court's Aereo decision, they should be entitled to a compulsory license under Section 111 of the copyright statute. The plaintiffs moved for summary judgment that the defendants did not qualify for the Section 111 license and that their nearly-simultaneous and time-delayed retransmission services violated the plaintiffs' public performance rights.⁵³⁶ For the reasons set forth in Section III.E.5(e) below, the court concluded that FilmOn X was not entitled to the Section 111 license.

The court also ruled that FilmOn X's service violated the plaintiffs' public performance rights. The defendants did not dispute that under the Supreme Court's Aereo decision FilmOn X's nearly-simultaneous retransmissions of over-the-air content were public performances for purposes of the Transmit Clause and therefore directly infringed the plaintiffs' rights of public performance. The court therefore turned to whether FilmOn's time-delayed service allowing individual subscribers to record over-the-air television programming and watch the selected content at a later time was also infringing.⁵³⁷

The defendants compared the service's storage and time-shifting function to that of cloud-based storage providers in which the user dictates what material will be stored on the network, when copies will be made, and when the network will transmit that data. The defendants argued that, since the individual user was the one who accessed the stored content and then directed the provider to transmit it, the process was nothing more than private transmission outside the scope of the Copyright Act. The court disagreed, finding that the Supreme Court's reasoning in Aereo confirmed the court's conclusion that the Transmit Clause encompassed FilmOn X's DVR-like functionality.⁵³⁸

⁵³⁵ Id. at 48-52.

⁵³⁶ Fox Televisions Stations, Inc. v. FilmOn X LLC, 150 F. Supp. 3d 1, 6-7 (D.D.C. 2015).

⁵³⁷ Id. at 30.

⁵³⁸ Id. at 30-31.

The court found that the defendants' arguments concerning private transmissions were essentially a rehash of Aereo's unsuccessful arguments before the Supreme Court in Aereo. The fact that the transmissions originated from individual copies and were streamed to individual users did not render the transmissions "private." Like its nearly-simultaneous transmission service, FilmOn X's DVR function rendered multiple subscribers capable of receiving the same perceptible images and sounds of over-the-air programs.⁵³⁹ Under Aereo, FilmOn X's transmissions were made to the public regardless of the time delay, because the Supreme Court had held that a transmission is performed publicly, regardless of whether the public is not situated together "spatially or temporally."⁵⁴⁰

The court also rejected the defendants' argument that FilmOn X could not be liable because they were not volitional actors with respect to their subscribers' retransmissions. The court found that in Aereo, the Supreme Court rejected the proposition that an entity such as FilmOn X is merely an equipment supplier that operates based on the subscriber's instruction and direction. An unauthorized secondary transmission constitutes a performance regardless of the time delay. In other words, just because the subscriber had to click a button to institute the streaming did not mean that FilmOn X did not perform within the meaning of the Transmit Clause. Finally, the court noted that the Supreme Court did not find it necessary to address the volitional conduct requirement to hold that both Aereo and its subscribers performed within the meaning of the Transmit Clause.⁵⁴¹

The district court further observed that for purposes of what constitutes a public performance, FilmOn X's service was much more similar to its nearly-simultaneous counterpart than to a cloud storage service. Unlike a cloud storage service, FilmOn X did not allow servers to store lawfully acquired content and play it back on command. Rather it captured broadcast signals and saved individual copies of the over-the-air content so that it could later stream the saved copy of the show to the subscriber over the Internet.⁵⁴² That difference was important because under the Supreme Court's Aereo decision "an entity that transmits a performance to individuals in their capacities as owners or possessors does not perform to 'the public,' whereas an entity like [FilmOn X] that transmits to large numbers of paying subscribers who lack any prior relationship to the works does so perform."⁵⁴³ Consequently, the district court rejected the defendants' repackaging of Aereo's unsuccessful arguments and ruled that Aereo's reasoning should be extended to FilmOn X's time-delayed retransmissions as direct violations of the plaintiffs' public performance rights.⁵⁴⁴

⁵³⁹ Id. at 31.

⁵⁴⁰ Id. (quoting Aereo, 134 S. Ct. at 2510).

⁵⁴¹ FilmOn X, 150 F. Supp. 3d at 31.

⁵⁴² Id. at 31-32.

⁵⁴³ Id. at 32 (quoting Aereo, 134 S. Ct. at 2510).

⁵⁴⁴ FilmOn X, 150 F. Supp. 3d at 32.

13. Hearst Stations v. Aereo

The case of Hearst Stations Inc. v. Aereo, Inc.⁵⁴⁵ was the fourth case (and the second against Aereo) to adjudicate claims of infringement of the public performance right based on a streaming and recording system utilizing individual mini digital antennas and DVRs to enable users to watch or record a free television broadcast. The plaintiff Hearst sought a preliminary injunction, arguing that Aereo's services fell within the definition of transmitting to the public – and therefore infringed its public performance rights – because Aereo was transmitting a performance of the *original* program to members of the public, and contended that the fact that each user viewed a unique copy of the program was irrelevant to the analysis. Aereo argued that it was transmitting private rather public performances per Cablevision. It also argued that Hearst's suggestion that the relevant performance was the copyrighted work read the terms "a performance or display" out of the statutory phrase "a performance or display of the work" in the transmit clause.⁵⁴⁶

The court ruled the following:

Aereo's interpretation is a better reading of the statute because the "canon against surplusage" requires this Court to give meaning to every statutory term if possible. See *Cablevision*, 536 F.3d at 135-36. The House Report accompanying the 1976 amendments, which explains that the process of communicating a copyrighted work from its original creator to the ultimate consumer may involve several "performances," provides further support. See H.R. Rep. No. 94-1476, at 63. In short, while the Transmit Clause is not a model of clarity, the Court finds at this juncture that Aereo presents the more plausible interpretation. As such, Hearst has not persuaded the Court that it is likely to succeed on the merits of its public performance claim.⁵⁴⁷

Hearst also argued that Aereo infringed its right of reproduction by creating and saving three copies of its copyrighted programming every time a consumer chose to watch or record a program. Aereo contended that it could not be liable for infringing the plaintiff's reproduction right because its users provided the volitional conduct that created the copy of the program they selected. The district court noted that the First Circuit had not yet decided whether a plaintiff claiming infringement of the reproduction right must show volitional conduct on the part of the defendant, but noted that courts in the Second, Third, and Fourth Circuit had imposed such a requirement. The court observed that requiring a showing of volitional conduct comports with the general principle that, even with a strict liability statute such as the Copyright Act, the challenged conduct must cause the harm. The court concluded that in this case it was likely that the user supplied the necessary volitional conduct to make the copy. The fact that Aereo users had the option to watch programs live did not command a different result because those users were informed that the system would create a copy of the program so they could pause and

⁵⁴⁵ 977 F. Supp. 2e 32 (D. Mass. 2013).

⁵⁴⁶ Id. at 38.

⁵⁴⁷ Id. at 38-39.

rewind. The court noted, however, that the reproduction issue was a closer question than the issue of public performance, and discovery could reveal that Aereo's service infringed the plaintiff's reproduction right.⁵⁴⁸

Hearst further contended that Aereo infringed its distribution right. The court noted that the Copyright Act does not define what it means to "distribute" but a number of courts had interpreted it to entail an actual dissemination of either copies or phonorecords. Here, because Aereo's technology allowed users only to stream but not download programming, Aereo was more aptly described as "performing" rather than "distributing" copyrighted works.⁵⁴⁹

Finally, Hearst contended that Aereo's act of reformatting intercepted programming violated its right to prepare derivative works. The court quickly dismissed this contention, noting that Hearst had presented no legal authority, nor was the court aware of any, for the proposition that Aereo's technology created a derivative work merely by converting programs from their original digital format to a different digital format compatible with Internet streaming. The court therefore denied the plaintiff's motion for a preliminary injunction.⁵⁵⁰

After the district court's decision, the Supreme Court issued its decision in the Aereo case, discussed in Section II.B.10 above, ruling that Aereo violated the public performance right by transmitting the plaintiffs' works through its system collectively to public subscribers. The Aereo decision undermines the district court's rulings in this case with respect to the public performance right.

14. Community Television of Utah v. Aereo

The case of Community Television of Utah, LLC v. Aereo, Inc.⁵⁵¹ was the fifth case (and the third against Aereo) to adjudicate claims of infringement of the public performance right based on a streaming and recording system utilizing individual mini digital antennas and DVRs to enable users to watch or record a free television broadcast. The plaintiffs sought a preliminary injunction, arguing that Aereo was violating their exclusive rights of public performance in their copyrighted broadcast programs. The court found that the plaintiffs were likely to succeed on the merits of their claim under the transmit clause, noting that the definitions pertinent to the transmit clause contained sweepingly broad language that easily encompassed Aereo's process of transmitting copyright-protected material to its paying customers. Specifically, the court found that Aereo used "any device or process" to transmit a performance or display of the plaintiffs' copyrighted programs to Aereo's paid subscribers, all of whom were members of the public who received it at the same time or separate times.⁵⁵²

⁵⁴⁸ Id. at 39.

⁵⁴⁹ Id. at 39-40.

⁵⁵⁰ Id. at 40-41.

⁵⁵¹ 997 F. Supp. 2d 1191 (D. Utah 2014).

⁵⁵² Id. at 1197-99.

To bolster its interpretation, the court reviewed the history of the adoption of the transmit clause, noting that Congress adopted it in response to two decisions of the Supreme Court under the 1909 Copyright Act⁵⁵³ holding that cable companies' erection of community antennas to receive broadcast signals and transmission of such signals to their subscribers' homes via coaxial cable did not violate the public performance right. In those cases the Supreme Court concluded that a cable company was free to do whatever a private citizen could do for itself without infringing a copyright. Congress then passed the transmit clause in part to abrogate the two Supreme Court decisions and bring a cable television system's transmission of broadcast television programming within the scope of the public performance right. The district court found that Aereo's retransmission of the plaintiffs' copyrighted programs was indistinguishable from a cable company and therefore fell squarely within the language of the transmit clause.⁵⁵⁴

The district court found the Second Circuit's interpretation of the transmit clause in the Cablevision case to be unpersuasive. The Second Circuit had focused on who was capable of *receiving* the performance in determining whether a performance was transmitted to the public. The district court found such a focus was not supported by the language of the statute, which states that it applies to any performance made *available* to the public. Aereo's paying subscribers to whom the performances were made available fell within the ambit of "a substantial number of persons outside of a normal circle of a family and its social acquaintances" and within a general understanding of the term "public."⁵⁵⁵ The court further criticized the reasoning of Cablevision as follows:

[T]he *Cablevision* court appears to discount the simple use of the phrase "to the public" because it concludes that the final clause within the Transmit Clause – "whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times" – was intended by Congress to distinguish between public and private transmissions. This court disagrees. The entire clause "whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times" appears to actually be Congress' attempt to broaden [the] scope of the clause, not an effort to distinguish public and private transmissions or otherwise limit the clause's reach. The term "whether" does not imply that the ensuing clause encompasses a limitation. Rather, the introduction of the clause with the word "whether" implies an intent to explain the broad sweep of the clause and the many different ways it could apply to members of the public. Reading this final clause

⁵⁵³ Fortnightly Corp. v. United Artists Television, Inc., 392 U.S. 390 (1968); Teleprompter Corp. v. Columbia Broadcasting Sys., 415 U.S. 394 (1974).

⁵⁵⁴ Community Television of Utah, 997 F. Supp. 2d at 1198-99.

⁵⁵⁵ Id. at 1200.

expansively is consistent with Congress' intent to have the entire Transmit Clause apply to all technologies developed in the future.⁵⁵⁶

Finally, the district court noted that the Second Circuit's analysis in Cablevision appeared to have erroneously changed the wording of the transmit clause from reading "members of the public capable of receiving the performance" to "members of the public capable of receiving the transmission." The court found that the language of the clause did not support a focus on who is capable of receiving a particular transmission. The court therefore found itself persuaded by Judge Chin's dissent in the Second Circuit's application of Cablevision to Aereo's system in WNET v. Aereo, discussed in Section II.B.10 above, when he concluded that, by any reasonable construction of the transmit clause, nothing Aereo was doing was in any sense "private" and Aereo was engaging in public performances when it intercepted and retransmitted copyrighted programs to paying strangers.⁵⁵⁷

The district court found the plaintiffs would suffer irreparable harm from Aereo's infringement by interfering with the plaintiffs' relationships and negotiations with legitimate licensees, impeding and affecting negotiations with advertisers, unfairly siphoning viewers from the plaintiffs' own web sites, threatening the plaintiffs' goodwill and contractual relationships with their licensed distributors, losing their position in the competitive marketplace for Internet content, and causing them to lose control of quality and potential piracy of their programming. The court also found the balance of harms to favor the plaintiffs and that a preliminary injunction would be in the public interest. Accordingly, the court granted the plaintiffs' motion for a preliminary injunction, but limited its scope to the region of the Tenth Circuit. The court ordered the plaintiffs to post a bond of \$150,000, and then stayed further proceedings in the case pending the Supreme Court's decision in American Broadcasting Corp. v. Aereo.⁵⁵⁸

Shortly after the district court's decision, the Supreme Court issued its decision in the case of American Broadcasting v. Aereo, discussed in Section II.B.10 above, ruling that Aereo violated the public performance right by transmitting the plaintiffs' works through its system collectively to public subscribers. That ruling substantively confirms the district court's outcome in this case.

15. CBS v. FilmOn

In 2010, CBS, NBC, Fox, and ABC brought an action for copyright infringement against FilmOn for streaming their broadcasting programming without their authorization. After completion of discovery, the parties settled the action and the court entered a consent order of judgment and permanent injunction dated Aug. 8, 2012, which prohibited FilmOn from further infringing plaintiffs' copyrights, including, but not limited to, through the streaming over mobile telephone systems and/or the Internet of any of the broadcast television programming in which

⁵⁵⁶ Id.

⁵⁵⁷ Id. at 1200-01.

⁵⁵⁸ Id. at 1203-04.

any plaintiff owned a copyright. In July of 2014 the plaintiffs moved the court for an order holding FilmOn and its CEO in civil contempt for violating the injunction by using mini-antenna technology (1) to broadcast the plaintiffs' copyrighted content within the Second Circuit in violation of the Supreme Court's decision in the Aereo case (discussed in Section II.B.10 above) and (2) to transmit such content to regions outside the Second Circuit through the use of FilmOn's "Teleporter" system, which allowed users to virtually view broadcast content from a distant location that was not necessarily within the local broadcast geographic region.⁵⁵⁹

FilmOn resisted the motion for contempt on the ground that, because the injunction did not expressly mention or prohibit the mini-antenna/DVR technology and the related Teleporter service, it could not be said to clearly and unambiguously prohibit its use. The court rejected this argument, noting that the injunction need not list every potential transmission mechanism that it barred in order to be clear and unambiguous. Recognizing the speed of technological advance, the injunction prohibited FilmOn from infringing by any means, and that was sufficiently clear to encompass FilmOn's antenna/DVR and Teleporter technology.⁵⁶⁰

FilmOn further argued that in light of the Supreme Court's findings in Aereo, it qualified as a cable system and was entitled to the benefits and responsibility of the compulsory license scheme under Section 111 of the Copyright Act. The court rejected this, noting that the Supreme Court's statements that Aereo (and, by extension, FilmOn, which used technology identical to Aereo) was very similar to a cable system were not the same as a judicial finding that Aereo and its technological peers are, in fact, cable companies entitled to retransmission licenses under Section 111. The district court further noted that the Supreme Court's Aereo decision did not mention, let alone abrogate, WPIX, Inc. v. ivi, Inc.,⁵⁶¹ which established the law in the Second Circuit that Internet retransmission services do not constitute cable systems under Section 111.⁵⁶²

The district court then turned to the factual support for finding FilmOn in contempt of the injunction. FilmOn had not stopped broadcasting the plaintiffs' content until it learned of the court's order to show cause in this case, twelve days after the Aereo decision, which the court found, at least as to the retransmissions within the Second Circuit, to constitute a clear violation of the injunction. Even assuming that FilmOn believed in good faith that the Aereo decision rendered it qualified to become a cable company under Section 111, it would nevertheless have needed to obtain a license from the Copyright Office in order to have been eligible to retransmit the plaintiff's content. FilmOn admitted that it had not even applied to the Copyright Office for such license until after the plaintiffs submitted their order to show cause,

⁵⁵⁹ CBS Broadcasting Inc. v. FilmOn.com, Inc., 2014 U.S. Dist. LEXIS 101894 at *1-3, *7 (S.D.N.Y. July 24, 2014). On Sept. 13, 2013, the court found FilmOn in contempt of the injunction by offering a video-on-demand service that provided subscribers with access to an archive of previously televised programs for streaming on demand. CBS Broadcasting Inc. v. FilmOn.com, Inc., 2013 U.S. Dist. LEXIS 130612 (S.D.N.Y. Sept. 10, 2013).

⁵⁶⁰ FilmOn, 2014 U.S. Dist. LEXIS 101894 at *9-10.

⁵⁶¹ 691 F.3d 275 (2d Cir. 2012), cert. denied, 133 S. Ct. 1585 (2013).

⁵⁶² FilmOn, 2014 U.S. Dist. LEXIS 101894 at *6, *11-12.

and the Copyright Office had subsequently issued a letter to FilmOn that, as an Internet retransmission service, it fell outside the scope of the Section 111 license, a conclusion that the Copyright Office believed Aereo did not alter.⁵⁶³

Accordingly, the court found both FilmOn and its CEO in violation of the injunction. FilmOn was ordered to pay \$10,000 for each of the nine days of its noncompliance pursuant to paragraph 3 of the 2012 consent order of judgment, plus a sanction of \$90,000.⁵⁶⁴

16. Capitol Records v. Escape Media

(For a discussion of public performance issues in this case, see Section III.C.1(c) below.)

17. Fox Broadcasting v. Dish Network

The facts of this case are discussed extensively in Section II.A.4(u) above. Pursuant to an agreement between Fox and Dish, Dish had the right to retransmit Fox programming to its subscribers via satellite as a pay television provider. In January of 2013 Dish introduced its second generation “Hopper” DVR set-top box called “Hopper with Sling” that had Sling technology (which transcoded video content from its source at the DVR set-top box and transmitted it to remote devices over the Internet) built into the box itself. In conjunction with the Hopper with Sling device, Dish rolled out a new service called Dish Anywhere, a mobile access application utilizing the Sling technology that allowed subscribers to watch live television or television programs recorded on the Hopper from any location on remote devices connected to the Internet. No copies were made to facilitate the remote viewing via Dish Anywhere. The content was transferred via Internet directly from the Hopper with Sling to the remote device and was not stored in and did not pass through any central server.⁵⁶⁵

Fox contended that Dish had publicly performed Fox’s copyrighted works by streaming them over the Internet to Dish subscribers using Dish Anywhere with Sling. Fox asserted that the Supreme Court’s decision in Aereo (discussed in Section II.A.4(aa) above) was a game-changer that governed the outcome of its copyright claims in this case. The district court disagreed. The district court noted that the Supreme Court did not expressly address the general volitional conduct requirement for direct liability in Aereo. Because the volitional conduct doctrine was a significant and long-standing rule, adopted by all Courts of Appeal to have considered it, the district court found that it would be folly to presume that Aereo categorically jettisoned it by implication.⁵⁶⁶

⁵⁶³ Id. at *14-17.

⁵⁶⁴ Id. at *19-20. The court found it unfair to hold FilmOn in contempt during the three-day period in which Aereo continued to stream content after the Supreme Court issued its Aereo decision. The court therefore found FilmOn’s noncompliance to begin on the day after Aereo stopped retransmitting content in the wake of Aereo and ended on the day FilmOn deactivated its mini-antenna service. Id. at *20 n.3.

⁵⁶⁵ Fox Broadcasting Co. v. Dish Network LLC, 160 F. Supp. 3d 1139, 1151, 1153-55 (C.D. Cal. 2015).

⁵⁶⁶ Id. at 1158-60.

Instead, the district court found that the majority analysis in Aereo could be reconciled with the volitional conduct requirement. The Aereo court had distinguished between an entity that engages in activities like Aereo's and one that merely supplies equipment that allows others to do so. Aereo held that a sufficient likeness to a cable company amounts to a presumption of direct performance, but the district court opined that the distinction between active and passive participation remains a central part of the analysis of an alleged infringement.⁵⁶⁷ Noting that the Aereo majority had relied on the fact that Aereo's system received programs that had been released to the public and carried them by private channels to additional viewers, the district court distinguished the instant case as follows:

DISH does not, however, receive programs that have been released to the public and then carry them by private channels to additional viewers in the same sense that Aereo did. DISH has a *license* for the analogous initial retransmission of the programming to users via satellite. Aereo streamed a subscriber-specific copy of its programming *from Aereo's hard drive* to the subscriber's screen via individual satellite when the subscriber requested it, whereas DISH Anywhere can only be used by a subscriber to gain access to *her own home STB/DVR* and the authorized recorded content on that box. Any subsequent transfer of the programming by DISH Anywhere takes place after the subscriber has validly received it, whereas Aereo transmitted its programming to subscribers directly, without a license to do so.⁵⁶⁸

The court summarized that the ultimate function of Dish Anywhere was to transmit programming that was already legitimately on a user's in-home hardware to a user's Internet-connected mobile device. Relying on external servers and equipment to ensure that content travelled between those devices properly did not transform that service into a traditional cable company. Aereo's holding that entities bearing an overwhelming likeness to cable companies publicly perform within the meaning of the transmit clause of the definition or "publicly perform" therefore did not extend to Dish Anywhere.⁵⁶⁹

The court then turned to the question whether, if any public performance occurred when subscribers used Dish Anywhere, Dish could be directly liable by virtue of engaging in sufficient volitional conduct enabling that performance. The court noted that, to use Dish Anywhere, a subscriber was required to log in or open the Dish Anywhere app, select the television program she wanted to watch, and request that the live or recorded television programming be sent from the set-top box in her home to her computer or mobile device. Although this process depended to some extent on external equipment and services provided by Dish, it was the user who initiated the process, selected the content, and received the transmission. The court therefore

⁵⁶⁷ Id. at 1160.

⁵⁶⁸ Id. at 1160-61 (citations omitted).

⁵⁶⁹ Id. at 1161.

concluded that Dish subscribers, not Dish, engaged in the volitional conduct necessary for any direct infringement.⁵⁷⁰

Finally, the court considered whether Dish might still be liable for secondary infringement if its subscribers were engaging in direct infringement by using Dish Anywhere to transmit public performances. The court concluded that the subscribers were not. Turning again to the Supreme Court’s Aereo decision, the district court noted that, in rejecting Aereo’s argument that it did not transmit a performance “to the public,” the Aereo opinion noted that nothing in the record before it suggested that the subscribers received the performances in their capacities as owners or possessors of the underlying works, and that this factor could affect whether or not the subscribers constituted “the public.” The district court noted that, in this case, Dish subscribers were valid possessors of the copyrighted works that were stored in the set-top boxes in their homes. Thus, when an individual Dish subscriber transmitted programming rightfully in her possession to another device, that transmission did not travel to a large number of people who are unknown to each other. Rather, the transmission travelled either to the subscriber herself or to someone in her household using an authenticated device. The court concluded that was simply not a “public” performance within the meaning of the transmit clause. Because Dish Anywhere subscribers did not directly infringe the public performance right, Dish could not be liable for secondary infringement, and the court therefore granted Dish’s motion for summary judgment as to the claim for copyright infringement by Dish Anywhere with Sling.⁵⁷¹

18. Disney Enterprises v. VidAngel

(For a discussion of public performance issues in this case, see Section III.G.1(a)(1)(xv) below.)

19. Spanski Enterprises v. Telewizja Polska

In this case the defendant, Poland’s national public television broadcaster, owned, operated and created content for a Polish language TV channel called TVP Polonia. The defendant entered into a licensing agreement with the plaintiff, a Canadian corporation, granting it exclusive broadcasting rights to TVP Polonia content in North and South America, including over the Internet. The plaintiff discovered that certain TVP Polonia content had not been properly geoblocked by the defendant, leaving it available to North and South American Internet users through the defendant’s video on demand system, including episodes that the plaintiff had registered with the U.S. Copyright Office and in which it held exclusive U.S. copyrights. The plaintiff sued asserting its exclusive right to perform the episodes. The district court found that the episodes were available and viewed in the U.S. because the defendant’s employees engaged in volitional action to remove the episodes’ default territorial restriction and created non-geoblocked digital formats of the episodes. The district court ruled that, by uploading such episodes on its foreign web site and directing the episodes to U.S. viewers upon their request, it

⁵⁷⁰ Id.

⁵⁷¹ Id. at 1162.

committed an infringing public performance under the U.S. copyright statute, that it was not protected from liability by the principle that copyright has no extraterritorial application, and that the plaintiff was entitled to statutory damages of \$60,000 per episode.⁵⁷²

On appeal, the D.C. Circuit affirmed. The defendant argued that it could not have liability under these circumstances because it had not engaged in volitional conduct, a requirement for direct infringement, in view of the fact that it was merely operating an automatic content delivery system that was not itself infringing and the user, not the defendant, selected the content the user would view or receive and actuated the delivery system, and the user request was not processed by the defendant's employees. The court rejected this argument, noting that nowhere does the copyright statute state that a work is publicly performed only if a third party end user plays no role in the showing. Here, because the defendant showed the copyrighted episodes to the public through its video on demand system – a device or process that rendered members of the public capable of receiving the performance in separate places and at different times – it had violated the plaintiff's public performance right.

And even apart from the statutory language, the court noted that the Supreme Court had held in the Aereo decision (discussed in Section II.B.10 above) that both the broadcaster and the viewer of a television program “perform,” because they both show the program's images and make audible the program's sounds. The Supreme Court further observed that an intermediary such as Aereo publicly performs even where its conduct consists only of capturing and retransmitting a broadcast in an automatic response to an end user's request. The Supreme Court concluded that a viewer's decision to access an infringing television program did not relieve a broadcaster from liability for showing the program's images and making audible the program's sounds. The D.C. Circuit noted that the defendant had offered no reason why the principles articulated in Aereo should fail to capture its conduct. Indeed, by selecting as well as transmitting copyrighted content, the D.C. Circuit found the defendant played an even more active role in broadcasting infringing performances than did Aereo.⁵⁷³

The D.C. Circuit further noted that it had yet to decide whether to read a volitional conduct or proximate cause requirement into the Copyright Act, and it need not do so in the present case. The defendant's conduct – using its own equipment to allow users to watch television programs, many of which were copyrighted, by transmitting content upon a user's request – constituted infringement under Aereo's binding authority, whatever the scope of any such volitional requirement might otherwise be. The court also rejected the defendant's reliance on Sony and Grokster, finding that neither decision had any clear relevance to this case. The defendant's argument that its video on demand system was broadly capable of non-infringing uses and was not created principally to induce infringement was beside the point. The defendant was being held liable for infringement not merely because it maintained a video on

⁵⁷² Spanski Enters. v. Telewizja Polska, S.A., 883 F.3d 904, 906-08 (D.C. Cir. 2018).

⁵⁷³ Id. at 910-12.

demand system, but rather because the defendant's own use of its system to communicate infringing performances amounted to actionable conduct under the Copyright Act.⁵⁷⁴

The court then turned to the extraterritoriality issue, noting that whether an infringing performance that originates abroad but that ultimately reaches viewers in the U.S. can be actionable under the Copyright Act was a question of first impression in the federal appellate courts. The court noted that, under applicable Supreme Court authority on extraterritoriality, in the absence of a clear, affirmative indication in a statute that it applies extraterritorially, a determination must be made whether the facts of the case, notwithstanding its extraterritorial elements, involve a permissible domestic application of the Copyright Act in view of the statute's focus, the objects of its solicitude, or what it is that the statute seeks to regulate or protect. In the case of the Copyright Act, the D.C. Circuit found its "focus" to be on protecting the exclusivity of the rights it guarantees. Here, although it was in Poland that the defendant uploaded and digitally formatted the episodes at issue, the infringing performance – and consequent violation of the plaintiff's copyrights – occurred on the computer screens in the U.S. on which the episodes' images were shown. Accordingly, because the conduct relevant to the statute's focus occurred in the U.S., this case involved a permissible domestic application of the Copyright Act, even if other conduct occurred abroad.⁵⁷⁵

The court rejected the defendant's argument that, based on the observation in Aereo that both the broadcaster and the viewer of a television program "perform" that program, there are *two* performances in the context of an international transmission – one by the broadcaster at the foreign point of origin and one by the user at the domestic point of reception. The court found that, under the defendant's reading, a broadcaster would commit an infringing performance merely by transmitting a copyrighted work into the void, regardless of whether that transmission ever resulted in the work's images being shown to even a single viewer. Given that the Copyright Act defines "perform" to require such a showing, the court ruled that Aereo is better read to establish only that a broadcaster and a viewer can *both* be liable for the *same* performance, i.e., the infringing display of copyrighted images on the viewer's screen. In this case, the infringing performance occurred in the U.S.⁵⁷⁶ In sum, the court held that, "where a foreign broadcaster uploads copyrighted content to its website and directs that content onto a computer screen in the United States at a user's request, the broadcaster commits an actionable domestic violation of the Copyright Act."⁵⁷⁷

C. The Right of Public Display

Section 106 (5) of the copyright statute grants the owner of copyright in a literary, musical, dramatic, and choreographic work, a pantomime, and a pictorial, graphic or sculptural

⁵⁷⁴ Id. at 912-13.

⁵⁷⁵ Id. at 913-14.

⁵⁷⁶ Id. at 914-15.

⁵⁷⁷ Id. at 918.

work, including the individual images of a motion picture or other audiovisual work,⁵⁷⁸ the exclusive right to display the work publicly.⁵⁷⁹ Section 101 defines the meaning of “to display a work publicly” in virtually identical terms as the definition of “to perform a work publicly.” Thus, a public display can be accomplished by a transmission of a display of the work to members of the public capable of receiving the display in the same place or separate places and at the same time or at different times.

The WIPO Copyright Treaty does not contain a right of public display per se. However, the right of public display is arguably subsumed under the right of communication to the public in the WIPO Copyright Treaty.

1. The Frena, Marobie-FL, Hardenburgh and Webbworld Cases

In Playboy Enterprises, Inc. v. Frena,⁵⁸⁰ the court held that the making of photographs available on a BBS was a “public” display, even though the display was limited to subscribers, and subscribers viewed the photographs only upon downloading the photographs from the BBS on demand. Thus, making material available through the Internet even to only a small and select audience may still constitute a “public” display. The point at which a selected audience becomes so small that a display to such audience can no longer be considered a “public” display is unclear. The Playboy court seemed to define an audience as “public” if it contains “a substantial number of persons outside of a normal circle of family and its social acquaintances.”⁵⁸¹

Similarly, in Marobie-FL, Inc. v. National Association of Fire Equipment Distributors,⁵⁸² the administrator of the Web page of the defendant, National Association of Fire Equipment Distributors (NAFED), placed certain files on NAFED’s Web page containing three volumes of copyrighted clip art of the plaintiff. The court ruled that the placement of the files containing the clip art on the Web page constituted a direct violation of both the plaintiff’s distribution right and public display right. The court concluded that the mere making available of the files for downloading was sufficient for liability, because “once the files were uploaded [onto the Web server], they were available for downloading by Internet users and ... the [OSP] server transmitted the files to some Internet users when requested.”⁵⁸³ The court, citing the Netcom case, refused to hold the OSP supplying Internet service to NAFED directly or vicariously liable, although the court noted that the OSP might be liable for contributory infringement, depending upon whether the OSP knew that any material on NAFED’s Web page was copyrighted, when it

⁵⁷⁸ To display a motion picture, one must display individual images “nonsequentially.” 17 U.S.C. § 101 (definition of “display”).

⁵⁷⁹ The right of public display does not apply to sound recordings, architectural works, and audiovisual works (except for display of individual images of an audiovisual work).

⁵⁸⁰ 839 F. Supp. 1552 (M.D. Fla. 1993).

⁵⁸¹ Id. at 1557.

⁵⁸² 45 U.S.P.Q.2d 1236 (N.D. Ill. 1997).

⁵⁸³ Id. at 1241.

learned of that fact, and the degree to which the OSP monitored, controlled, or had the ability to monitor or control the contents of NAFED's Web page.⁵⁸⁴

And in Playboy Enterprises, Inc. v. Hardenburgh,⁵⁸⁵ the defendants operated a BBS which made available graphic image files to subscribers for a fee, many of which contained adult material. To increase its stockpile of available information, and thereby its attractiveness to new customers, defendants provided an incentive to encourage subscribers to upload information onto the BBS. Subscribers were given "credit" for each megabyte of electronic data that they uploaded onto the system, which entitled them to download defined amounts of data from the system in return. Information uploaded onto the BBS went directly to an "upload file" where an employee of the BBS briefly checked the new files to ascertain whether they were "acceptable," meaning not pornographic and not blatantly protected by copyright.⁵⁸⁶ Many of the plaintiff's copyrighted photographs appeared on the BBS and the plaintiff brought suit for infringement.

With respect to the issue of direct liability for the infringing postings of its subscribers, the court agreed with the Netcom decision's requirement of some direct volitional act or participation in the infringement. However, the court found that the facts of the case, unlike those of Frena, MAPHIA, and Netcom, were sufficient to establish direct liability for infringement of both the public display and distribution rights. The court based its conclusion on "two crucial facts: (1) Defendants' policy of encouraging subscribers to upload files, including adult photographs, onto the system, and (2) Defendants' policy of using a screening procedure in which [its] employees viewed all files in the upload file and moved them into the generally available files for subscribers. These two facts transform Defendants from passive providers of a space in which infringing activities happened to occur to active participants in the process of copyright infringement."⁵⁸⁷

Finally, in Playboy Enterprises, Inc. v. Webbworld, Inc.,⁵⁸⁸ the court held the defendants directly liable for infringing public displays of copyrighted images for making such images available through a website for downloading by subscribers.

2. Kelly v. Arriba Soft

An important case construing the scope of the public display right on the Internet is that of Kelly v. Arriba Soft Corp.⁵⁸⁹ In that case, the defendant Arriba was the operator of a "visual search engine" on the Internet that allowed users to search for and retrieve images. In response to a search query, the search engine produced a list of reduced, "thumbnail" images. To provide

⁵⁸⁴ Id. at 1245.

⁵⁸⁵ 982 F. Supp. 503 (N.D. Ohio 1997).

⁵⁸⁶ Id. at 506.

⁵⁸⁷ Id. at 513.

⁵⁸⁸ 45 U.S.P.Q.2d 1641 (N.D. Tex. 1997).

⁵⁸⁹ 336 F.3d 811 (9th Cir. 2003).

this functionality, Arriba developed a program called a “crawler” that would search the Web looking for images to index, download full-sized copies of the images onto Arriba’s server, then use those images to generate lower resolution thumbnails. Once the thumbnails were created, the program deleted the full-sized originals from the server.⁵⁹⁰

When the user double-clicked on the thumbnail, a full-sized version of the image was displayed. During one period of time, the full-sized images were produced by “inline linking” (or “inlinks”) – i.e., by retrieving the image from the original web site and displaying it on the Arriba web page with text describing the size of the image and a link to the originating site – such that the user would typically not realize the image actually resided on another web site. During a subsequent period of time, the thumbnails were accompanied by two links, a “source” and a “details” link. The “details” link produced a separate screen containing the thumbnail image with text describing the size of the image and a link to the originating site. Alternatively, by clicking on the “source” link or the thumbnail itself, the Arriba site produced two framed windows on top of the Arriba page: the window in the forefront contained the full-sized image, imported directly from the originating site; underneath that was a second window displaying the home page containing the image from the original site.⁵⁹¹

Arriba’s crawler copied 35 photographs on which the plaintiff, Kelly, held the copyrights into the Arriba database. When he complained, Arriba deleted the thumbnails of images that came from Kelly’s own web sites and placed those sites on a list of sites that it would not crawl in the future. Several months later, Kelly sued Arriba, identifying in the complaint other images of his that came from third party web sites.⁵⁹² The district court ruled that Arriba’s use of both the thumbnails and the full sized images was a fair use, and Kelly appealed.⁵⁹³

The Ninth Circuit, in an opinion issued in July of 2003,⁵⁹⁴ affirmed the ruling that the use of the thumbnails was a fair use. Applying the first of the four statutory fair use factors, the court held that the thumbnails were a transformative use of Kelly’s works because they were much smaller, lower resolution images that served an entirely different function than Kelly’s original images. Users would be unlikely to enlarge the thumbnails and use them for artistic purposes because the thumbnails were of much lower resolution than the originals. Thus, the first fair use factor weighted in favor of Arriba.⁵⁹⁵

The court held that the second factor, the nature of the copyrighted work, weighed slightly in favor of Kelly because the photographs were creative in nature. The third factor, the

⁵⁹⁰ Id. at 815.

⁵⁹¹ Id. at 815-16.

⁵⁹² Id. at 816.

⁵⁹³ Id. at 816-17.

⁵⁹⁴ The 2003 opinion withdrew an earlier and highly controversial opinion issued by the court in 2002, discussed further below.

⁵⁹⁵ Id. at 818-19.

amount and substantiality of the portion used, was deemed not to weigh in either party's favor. Although the entire images had been copied, it was necessary for Arriba to copy the entire images to allow users to recognize the image and decide whether to pursue more information about it or the originating web site.⁵⁹⁶

Finally, the court held that the fourth factor, the effect of the use upon the potential market for or value of the copyrighted work, weighed in favor of Arriba. The court found that Arriba's use of the thumbnail images would not harm the market for Kelly's use of his images or the value of his images. By displaying the thumbnails, the search engine would guide users to Kelly's web site rather than away from it. Nor would Arriba's use of the images harm Kelly's ability to sell or license the full-sized images. Anyone downloading the thumbnails would not be successful selling full sized-images from them because of the low resolution of the thumbnails, and there would be no way to view, create, or sell clear, full-sized images without going to Kelly's web sites. Accordingly, on balance, the court found fair use.⁵⁹⁷

The court reversed, however, the district court's ruling that Arriba's use of the full-sized images through inline linking or framing was a fair use and remanded for further proceedings. The Ninth Circuit's ruling on this issue was contrary to a result the Ninth Circuit had reached in an earlier opinion in the case issued in 2002,⁵⁹⁸ which it withdrew when issuing its 2003 opinion. In the 2002 ruling, the Ninth Circuit had held, in a highly controversial ruling, that Arriba's inline linking to and framing of the full-sized images violated the plaintiff's public display rights.⁵⁹⁹ Interestingly, the court ruled that Kelly's reproduction rights had not been infringed: "This use of Kelly's images does not entail copying them but, rather, importing them directly from Kelly's web site. Therefore, it cannot be copyright infringement based on the reproduction of copyrighted works Instead, this use of Kelly's images infringes upon Kelly's exclusive right to 'display the copyrighted work publicly.'"⁶⁰⁰ Apparently the court's observation that the offering of the full-sized images through linking "does not entail copying" was meant to refer to direct copying by Arriba, because a copy of the images is certainly made in the user's computer RAM, as well as on the screen, when the user clicks on the thumbnail to display the full sized image.

With respect to infringement of the display right, the court ruled in its 2002 opinion that the *mere act of linking* to the images constituted infringement. First, the court ruled that there was an unauthorized "display": "By inline linking and framing Kelly's images, Arriba is showing Kelly's original works without his permission."⁶⁰¹ Second, the court held that such "showing" was a "public" one: "A display is public even if there is no proof that any of the potential

⁵⁹⁶ Id. at 820-21.

⁵⁹⁷ Id. at 821-22.

⁵⁹⁸ Kelly v. Arriba Soft Corp., 280 F.3d 934 (9th Cir. 2002).

⁵⁹⁹ Kelly had never argued, either in the proceedings below or on appeal, that his public display rights had been infringed. The Ninth Circuit raised this issue on its own.

⁶⁰⁰ Id. at 944.

⁶⁰¹ Id. at 945.

recipients was operating his receiving apparatus at the time of the transmission. By making Kelly's images available on its web site, Arriba is allowing public access to those images. The ability to view those images is unrestricted to anyone with a computer and internet access."⁶⁰² The court thus concluded that Arriba had directly infringed Kelly's public display rights: "By allowing the public to view Kelly's copyrighted works while visiting Arriba's web site, Arriba created a public display of Kelly's works. ... Allowing this capability is enough to establish an infringement; the fact that no one saw the images goes to the issue of damages, not liability."⁶⁰³

The court went on in its 2002 opinion to hold that Arriba's display of Kelly's full-sized images was not a fair use. Unlike the case of the thumbnails, the court held that the use of the full-sized images was not transformative. "Because the full-sized images on Arriba's site act primarily as illustrations or artistic expression and the search engine would function the same without them, they do not have a purpose different from Kelly's use of them."⁶⁰⁴ Accordingly, the first factor weighed against fair use. For the same reasons as before, the second factor weighed slightly in favor of Kelly.⁶⁰⁵ The third factor weighed in favor of Kelly because, although it was necessary to provide whole images "to suit Arriba's purpose of giving users access to the full-sized images without having to go to another site, such a purpose is not legitimate."⁶⁰⁶ Finally, the fourth factor weighed in Kelly's favor, because "[b]y giving users access to Kelly's full-sized images on its own web site, Arriba harms all of Kelly's markets."⁶⁰⁷

The Ninth Circuit's ruling in its 2002 decision on the public display issue generated a lot of controversy, since the reach of that ruling was potentially so broad. In particular, the logic the Ninth Circuit adopted in its 2002 decision – that the mere act of inline linking to or framing of a work, whether or not users actually view the linked work – constitutes a public display of the linked work, could call into question the legality of many types of linking or framing that has not been expressly authorized by the owner of the linked material. Apparently in response to the controversy, on Oct. 10, 2002, the Ninth Circuit ordered additional briefing on issues of public display and derivative use rights raised by the case.⁶⁰⁸

In its 2003 decision, the Ninth Circuit omitted entirely the discussion of the public display right that had appeared in its 2002 decision. Instead, the court held that the district court should not have decided whether the display of the full-sized images violated Kelly's public display rights because the parties never moved for summary judgment on that issue.⁶⁰⁹ In the

⁶⁰² Id.

⁶⁰³ Id. at 946.

⁶⁰⁴ Id. at 947.

⁶⁰⁵ Id. at 947-48.

⁶⁰⁶ Id. at 948.

⁶⁰⁷ Id.

⁶⁰⁸ "Ninth Circuit Orders Added Briefs on Hyperlinking Issues in Arriba Soft Appeal," *BNA's Electronic Commerce & Law Report* (Oct. 30, 2002) at 1082.

⁶⁰⁹ Kelly v. Arriba Soft Corp., 336 F.3d 811, 822 (9th Cir. 2003).

proceedings below, Kelly had moved only for summary judgment that Arriba's use of the thumbnail images violated his display, reproduction and distribution rights. Arriba cross-moved for summary judgment and, for purposes of the motion, conceded that Kelly had established a prima facie case of infringement as to the thumbnail images, but argued that its use of the thumbnail images was a fair use. The Ninth Circuit concluded that, by ruling that use of both the thumbnail images and the full-sized images was fair, the district court had improperly broadened the scope of both Kelly's original motion to include a claim for infringement of the full-sized images and the scope of Arriba's concession to cover the prima facie case for both the thumbnail images and the full-sized images.⁶¹⁰ Accordingly, the court remanded for further proceedings with respect to the full-sized images to give the parties an opportunity to fully litigate those issues.⁶¹¹

3. Ticketmaster v. Tickets.com

See Section III.D.7 below for a discussion of this case, which distinguished the Kelly v. Arriba Soft case and held that Tickets.com's deep linking to pages on Ticketmaster's web site where tickets could be purchased for events listed on Tickets.com's site did not constitute an infringing public display.

4. Perfect 10 v. Google (aka Perfect 10 v. Amazon)

Perfect 10 v. Google set forth a detailed adjudication of the boundaries of the display right on the Internet, and in particular, which entity should be deemed to perform the display for purposes of copyright liability when the display results through links from a web site to another web site storing copies of the copyrighted material at issue. Because both the district court and the Ninth Circuit issued very thorough, thoughtful opinions, the holdings of both courts will be explained in detail.

The plaintiff Perfect 10 sought to preliminarily enjoin Google from displaying thumbnails and full size versions of its copyrighted photographs through the "Google Image Search" function in response to user search queries. Google Image Search allowed a user to input a text search string and returned thumbnail images organized into a grid potentially responsive to the search query.⁶¹²

To operate Google Image Search, Google created and stored in its cache thumbnail versions of images appearing on web sites crawled by Google's web crawler. The thumbnails chosen for display in response to search queries depended solely upon the text surrounding the image at the original site from which the image was drawn. When a user clicked on a thumbnail image, Google displayed a page comprised of two distinct frames divided by a gray horizontal

⁶¹⁰ Id. at 817.

⁶¹¹ Id. at 822.

⁶¹² Perfect 10 v. Google, 416 F. Supp. 2d 828, 832-33 (C.D. Cal. 2006), aff'd sub nom. Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1169 (9th Cir. 2007).

line, one frame hosted by Google and the second one hosted by the underlying web site that originally hosted the full size image.⁶¹³ In the upper frame, Google displayed the thumbnail, retrieved from its cache, and information about the full size image, including the original resolution of the image and the specific URL associated with that image. The upper frame made clear that the image might be subject to copyright and that the upper frame was not the original context in which the full size image was found. The lower frame contained the original web page on which the original image was found. Google neither stored nor served any of the content displayed in the lower frame, which was stored and served by the underlying third party web site containing the original image.⁶¹⁴ Perfect 10 brought claims against Google for direct, vicarious and contributory copyright infringement.

Direct Infringement Claims. Perfect 10 alleged that Google directly infringed its copyrights by displaying and distributing the full size images hosted by third party web sites, and by creating, displaying and distributing thumbnails of its copyrighted full size images. Google conceded that it created and displayed thumbnails, but denied that it displayed, created, or distributed what was depicted in the lower frame of search results displays, which were generated via inline links to third party sites storing the original images of interest.⁶¹⁵

The district court began with a consideration of how “display” should be defined in the context of inline linking, noting that two approaches were possible: (1) a “server test,” in which display is defined as the act of *serving* content over the web, i.e., physically sending bits over the Internet to the user’s browser, and (2) an “incorporation” test, in which display is defined as the mere act of incorporating content into a web page that is then pulled up by the browser through an inline link. Under the server test, advocated in the case by Google, the entity that should be deemed liable for the display of infringing content is the entity whose server served up the infringing material. Under the incorporation test, advocated by Perfect 10, the entity that should be deemed liable for the display of infringing content is the entity that uses an inline link in its web page to direct the user’s browser to retrieve the infringing content.⁶¹⁶

The district court reviewed the existing decisions dealing with the question of whether linking constitutes infringing “displaying” of copyrighted material. The court noted that in the Webbworld and Hardenburg cases,⁶¹⁷ the material was stored on the defendant’s servers, and in the Perfect 10 v. Cybernet Ventures case,⁶¹⁸ it was unclear whether the defendant stored or served any of the infringing content. The court further noted that the Ninth Circuit had withdrawn its opinion in Kelly v. Arriba Soft⁶¹⁹ adopting the incorporation test in the face of

⁶¹³ Id. at 833.

⁶¹⁴ Id. at 833-34.

⁶¹⁵ Id. at 838.

⁶¹⁶ Id. at 838-40.

⁶¹⁷ These cases are discussed in Section II.C.1 above.

⁶¹⁸ This case is discussed in Section II.A.4(k) above.

⁶¹⁹ This case is discussed in Section II.C.2 above.

widespread criticism of that decision. The court therefore found that none of these cases, or any other existing precedent, resolved the question before it.⁶²⁰

The district court concluded that the server test was the most appropriate one for determining whether Google's lower frames were a "display" of infringing material. The court articulated several reasons for adopting the server test. First, it is based on what happens at the technological level as users browse the web, and thus reflects the reality of how content actually travels over the Internet before it is shown on users' computers. Second, it precludes search engines from being held directly liable for inline linking and/or framing infringing content stored on third party web sites, but allows copyright owners still to seek to impose contributory or vicarious liability on web sites for including such content. Third, web site operators can readily understand the server test and courts can apply it relatively easily. Fourth, in the instant case, it imposes direct liability on the web sites that took Perfect 10's full size images and posted them on the Internet for all to see. Finally, the server test promotes the balance of copyright law to encourage the creation of works by protecting them while at the same time encouraging the dissemination of information. The server test would avoid imposing direct liability for merely indexing the web so that users can more readily find the information they seek, while imposing direct liability for the hosting and serving of infringing content.⁶²¹

Applying the server test, the district court ruled that for purposes of direct infringement, Google's use of frames and inline links did not constitute a "display" of the full size images stored on and served by infringing third party web sites, but Google did "display" the thumbnails of Perfect 10's copyrighted images because it created, stored, and served those thumbnails on its own servers.⁶²²

On appeal, the Ninth Circuit agreed with the district court that the server test should be used to determine which entity displays an image on the web, concluding that the test was consistent with the statutory language of the copyright statute. Under that test, Perfect 10 had made a prima facie case that Google's communication of its stored thumbnail images directly infringed Perfect 10's display rights. However, Google had not publicly displayed a copy of the full size infringing images when it framed inline linked images that appeared on a user's computer screen.⁶²³ The Ninth Circuit found that Google's activities with respect to the full size images did not meet the statutory definition of public display "because Google transmits or communicates only an address which directs a user's browser to the location where a copy of the full-size image is displayed. Google does not communicate a display of the work itself."⁶²⁴

⁶²⁰ 416 F. Supp. 2d at 840-43.

⁶²¹ Id. at 843-44.

⁶²² Id. at 844.

⁶²³ Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1159-60 (9th Cir. 2007).

⁶²⁴ Id. at 1161 n.7.

The court also ruled that, because Google's cache merely stored the text of web pages, and not the images themselves, Google was not infringing the display right by virtue of its cache.⁶²⁵

Fair Use. The district court evaluated Google's assertion of the fair use defense to the display of the thumbnails. With respect to the first fair use factor, the purpose and character of the use, the court found that Google's display of the thumbnails was a commercial use, since Google derived significant commercial benefit from Google Image Search in the form of increased user traffic and, in turn, increased advertising revenue. The court distinguished the Ninth Circuit's decision in the Kelly v. Arriba Soft case by noting that, unlike Arriba Soft, Google derived direct commercial benefit from the display of thumbnails through its "AdSense" program, under which third party web sites could place code on their sites to request Google's server to algorithmically select relevant advertisements for display based on the content of the site, and then share revenue flowing from the advertising displays and click-throughs. If third party web sites participating in the AdSense program contained infringing copies of Perfect 10 photographs, Google would serve ads on those sites and split the revenue generated from users who clicked on the Google-served ads.⁶²⁶ Accordingly, the court concluded that "AdSense unquestionably makes Google's use of thumbnails on its image search far more commercial than Arriba's use in *Kelly II*. Google's thumbnails lead users to sites that directly benefit Google's bottom line."⁶²⁷

Relying on the Kelly v. Arriba Soft decision, the court concluded that the use of the thumbnails was transformative because their creation and display enabled the display of visual search results quickly and efficiently, and did not supersede Perfect 10's use of the full size images. But the court noted that the transformative nature of the thumbnail use did not end the analysis, because the use was also "consumptive." In particular, the court noted that after it filed suit against Google, Perfect 10 entered into a licensing agreement with a third party for the sale and distribution of Perfect 10 reduced-size images for download to and use on cell phones.⁶²⁸ "Google's use of thumbnails does supersede this use of P10's images, because mobile users can download and save the thumbnails displayed by Google Image Search onto their phones."⁶²⁹ On balance, then, the court concluded that, because Google's use of thumbnails was more commercial than Arriba Soft's and because it was consumptive with

⁶²⁵ Id. at 1162.

⁶²⁶ Perfect 10 v. Google, 416 F. Supp. 2d 828, 834, 846-47 (C.D. Cal. 2006), aff'd sub nom. Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1169 (9th Cir. 2007).

⁶²⁷ Id. at 846. Google counterargued that its AdSense program policies prohibited a web site from registering as an AdSense partner if the site's web pages contained images that appeared in Google Image Search results. The court noted, however, that Google had not presented any information regarding the extent to which the purported policy was enforced nor had it provided examples of AdSense partners who were terminated because of violations of the policy. In contrast, Perfect 10 submitted numerous screenshots of third party web sites that served infringing content and also appeared to be receiving and displaying AdSense ads from Google. Id. at 846-47.

⁶²⁸ Id. at 847-49.

⁶²⁹ Id. at 849.

respect to Perfect 10's reduced-size images, the first factor weighed "slightly in favor" of Perfect 10.⁶³⁰

The district court ruled that the second fair use factor, the nature of the copyrighted work, weighed "only slightly in favor" of Perfect 10 because, although its photographs were creative, as in the case of the Kelly v. Arriba Soft case, they had appeared on the Internet before use in Google's search engine.⁶³¹ The court found that the third factor, the amount and substantiality of the portion used, favored neither party because Google's use of the copies of Perfect 10's images was no greater than necessary to achieve the objective of providing effective image search capabilities.⁶³² Finally, the court found that the fourth factor, the effect of the use upon the potential market for and value of the copyrighted work, weighed slightly in Perfect 10's favor because of the court's finding that Google's use of thumbnails likely would harm the potential market for the downloading of Perfect 10's reduced-size images onto cell phones. On balance, then, the court found that the fair use doctrine likely would not cover Google's use of the thumbnails.⁶³³

On appeal, the Ninth Circuit reached the opposite conclusion under the fair use doctrine. Before beginning its specific analysis of the four fair use factors, the Ninth Circuit made some important preliminary rulings concerning the burden of proof with respect to the fair use doctrine. The district court had ruled that, because Perfect 10 had the burden of showing a likelihood of success on the merits, it also had the burden of demonstrating a likelihood of overcoming Google's fair use defense. The Ninth Circuit held the district court's ruling on this point to be erroneous. Citing cases from the Supreme Court and the Federal Circuit holding that the burdens at the preliminary injunction stage track the burdens at trial, the Ninth Circuit ruled that, once Perfect 10 had shown a likelihood of success on the merits, the burden shifted to Google to show a likelihood that its affirmative defenses – including that of fair use – would succeed.⁶³⁴

⁶³⁰ Id.

⁶³¹ Id. at 849-50.

⁶³² Id. at 850.

⁶³³ Id. at 850-51.

⁶³⁴ Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1158 (9th Cir. 2007). This holding was the opposite of one the Ninth Circuit had reached in an earlier issued opinion in the appeal, which the instant opinion replaced. In the earlier opinion, the Ninth Circuit had concluded that, because a plaintiff has the burden of showing a likelihood of success on the merits in order to obtain a preliminary injunction, the plaintiff should also have the burden of demonstrating a likelihood of overcoming the defendant's fair use defense. However, because the defendant in an infringement action has the burden of proving fair use, the Ninth Circuit had ruled in its earlier opinion that the defendant is responsible for introducing evidence of fair use in the first instance in responding to a motion for preliminary relief, whereupon the burden would then shift to the plaintiff to demonstrate that it will overcome the fair use defense. Perfect 10 v. Amazon.com, Inc., 487 F.3d 701, 714 (9th Cir. 2007) (superseded by 508 F.3d 1146 (9th Cir. 2007)). The court further elaborated its rationale in the earlier opinion as follows: "In order to demonstrate its likely success on the merits, the moving party must necessarily demonstrate it will

The Ninth Circuit's analysis of the fair use factors is significant in its recognition of the need, when judging the transformative nature of the use, to balance the public benefit from the use against the potential harm to the rights holder from superseding commercial uses, as well as in its requirement of a showing that alleged potential superseding commercial uses are both real and significant in their impact. Specifically, with respect to the first factor, the Ninth Circuit, citing the Kelly v. Arriba Soft case, noted that Google's use of the thumbnails was highly transformative because its search engine transformed each image into a pointer directing a user to a source of information.⁶³⁵ In addition, "a search engine provides social benefit by incorporating an original work into a new work, namely, an electronic reference tool."⁶³⁶

In a significant ruling, the Ninth Circuit disagreed, on two grounds, with the district court's conclusion that Google's use of thumbnail images was less transformative than the video search engine at issue in Kelly v. Arriba Soft because Google's use of thumbnails superseded Perfect 10's right to sell its reduced-size images for use on cell phones. First, the Ninth Circuit noted that the alleged superseding use was not significant at the present time, because the district court had not found that any downloads of Perfect 10's photos for mobile phone use had actually taken place.⁶³⁷ Second, the court concluded "that the significantly transformative nature of Google's search engine, particularly in light of its public benefit, outweighs Google's superseding and commercial uses of the thumbnails in this case."⁶³⁸ Accordingly, the first fair use factor weighed in favor of Google.

The Ninth Circuit found that the district court had correctly analyzed the second and third factors.⁶³⁹ With respect to the fourth factor, Perfect 10 challenged the district court's finding of no harm to the market for the full sized images on the ground that likelihood of market harm may be presumed if the intended use of an image is for commercial gain. The court noted, however, that this presumption does not arise when a work is transformative because market substitution is less certain. Because Google's use of thumbnails for search

overcome defenses raised by the non-moving party. This burden is correctly placed on the party seeking to demonstrate entitlement to the extraordinary remedy of a preliminary injunction at an early stage of the litigation, before the defendant has had the opportunity to undertake extensive discovery or develop its defenses." 487 F.3d at 714. The Ninth Circuit apparently concluded that this earlier holding was inconsistent with established precedent that the burdens at the preliminary injunction stage track the burdens at trial, leading the court to issue a revised opinion.

⁶³⁵ 508 F.3d at 1165.

⁶³⁶ Id. The Ninth Circuit rejected Perfect 10's argument that providing access to infringing web sites cannot be deemed transformative and is inherently not fair use. The court noted that Google was operating a comprehensive search engine that only incidentally indexed infringing web sites. "This incidental impact does not amount to an abuse of the good faith and fair dealing underpinnings of the fair use doctrine. Accordingly, we conclude that Google's inclusion of thumbnail images derived from infringing websites in its Internet-wide search engine activities does not preclude Google from raising a fair use defense." Id. at 1164 n.8.

⁶³⁷ Id. at 1166.

⁶³⁸ Id.

⁶³⁹ Id. at 1167-68.

engine purposes was highly transformative and market harm could therefore not be presumed, and because Perfect 10 had not introduced evidence that Google's thumbnails would harm its existing or potential market for full size images, the Ninth Circuit rejected Perfect 10's argument.⁶⁴⁰

With respect to harm to Perfect 10's alleged market for reduced size images, the Ninth Circuit noted that the district court did not make a finding that Google users had actually downloaded thumbnail images for cell phone use, so any potential harm to that alleged market remained hypothetical. Accordingly, the court concluded that the fourth factor favored neither party.⁶⁴¹ Balancing the four factors, and particularly weighing Google's highly transformative use and its public benefit against the unproven use of thumbnails for cell phone downloads, the court concluded that Google's use of Perfect 10's thumbnails was a fair use. Accordingly, the court vacated the preliminary injunction regarding Google's use of thumbnail images.⁶⁴²

Contributory Infringement. Perfect 10 argued to the district court that Google was contributing to the infringement of two direct infringers – third party web sites hosting and serving infringing copies of Perfect 10 photographs, and Google Image Search users downloading such images. The district court ruled as a preliminary matter that Perfect 10 could not base its contributory infringement claim on users' actions, because Perfect 10 had demonstrated only that users of Google search were *capable* of directly infringing by downloading the images, but had not submitted sufficient evidence showing the extent to which users were in fact downloading Perfect 10's images through Google Image Search. Thus, the contributory infringement claim had to be based on knowledge and material contribution by Google to the infringing activities of third party web sites hosting Perfect 10's images.⁶⁴³

With respect to the knowledge prong, the district court, citing the Supreme Court's Grokster case, noted that either actual or constructive knowledge is sufficient for contributory liability. The court rejected Perfect 10's argument that Google had actual knowledge from the presence of copyright notices on Perfect 10's images or from the fact that Google's AdSense policy stated that it monitored the content of allegedly infringing sites. The court noted that Google would not necessarily know that any given image on the Internet was infringing someone's copyright merely because the image contained a copyright notice. With respect to the alleged monitoring by Google, Google had changed its AdSense policy to remove the language reserving to Google the right to monitor its AdSense partners. The court further noted

⁶⁴⁰ Id. at 1168.

⁶⁴¹ Id.

⁶⁴² Id. In a side, but significant, issue, Google argued that the Ninth Circuit lacked jurisdiction over the preliminary injunction to the extent it enforced unregistered copyrights. The court rejected this argument: "Once a court has jurisdiction over an action for copyright infringement under section 411 [of the copyright statute], the court may grant injunctive relief to restrain infringement of any copyright, whether registered or unregistered." Id. at 1154 n.1.

⁶⁴³ Perfect 10 v. Google, 416 F. Supp. 2d 828, 851-52 (C.D. Cal. 2006), aff'd sub nom. Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1169 (9th Cir. 2007).

that, in any event, merely because Google may have reserved the right to monitor its AdSense partners did not mean that it could thereby discern whether the images served by those web sites were subject to copyright.⁶⁴⁴

The district court then turned to an analysis of whether numerous notices of infringement sent by Perfect 10 to Google were sufficient to give Google actual knowledge of infringing activity. Google challenged the adequacy of those notices on the grounds that they frequently did not describe in sufficient detail the specific URL of an infringing image and frequently did not identify the underlying copyrighted work. Some notices listed entire web sites as infringing, or entire directories within a web site. Google claimed that despite these shortcomings, it promptly processed all of the notices it received, suppressing links to specific web pages that it could confirm displayed infringing Perfect 10 copies. The court concluded, however, that it need not resolve the question of whether Google had adequate actual knowledge of infringement, in view of the court's conclusion that Google had not materially contributed to the infringing activity of third party web sites.⁶⁴⁵

The district court articulated the following grounds for its finding that Perfect 10 had not adequately met its burden to show that Google sufficiently contributed to the infringing activity for contributory liability. First, the court set forth numerous differences between Google's activity and the activity that had been found to materially contribute to infringement in the Napster cases. For example, unlike in the case of the Napster system, in the instant case the infringing third party web sites existed, were publicly accessible, and engaged in the infringing activity irrespective of their inclusion or exclusion from Google's index. Unlike Napster, Google did not provide the means of establishing connections between users' computers to facilitate the downloading of the infringing material. Even absent Google, third party web sites would continue to exist and would continue to display infringing content (an observation which would seem true of all search engines). And unlike Napster, Google did not boast about how users could easily download infringing content, nor did it facilitate the transfer of files stored on users' otherwise private computers.⁶⁴⁶

In sum, the district court found that Perfect 10 had overstated Google's actual conduct and confused the mere provision of search technology with active encouragement and promotion of infringing activity. The court also rejected Perfect 10's argument based on the Supreme Court's Grokster case that Google had materially contributed to the infringing activity by providing through AdSense a revenue stream to the infringing web sites. The court held that, although the AdSense program might provide some level of additional revenue to the infringing web sites, Perfect 10 had not presented any evidence establishing what that revenue was, much less that it was material, either in its own right or relative to those web sites' total income.

⁶⁴⁴ Id. at 853-54.

⁶⁴⁵ Id. at 854.

⁶⁴⁶ Id.

Accordingly, the court ruled that Perfect 10 was not likely to prevail on its claim for contributory liability.⁶⁴⁷

In an important ruling on appeal,⁶⁴⁸ the Ninth Circuit reversed and remanded for factual findings under a specialized test for contributory infringement for computer system operators. The Ninth Circuit began its analysis by examining the issue of whether Perfect 10 had adequately proved direct infringements to which Google could potentially contribute. Perfect 10 alleged that three parties directly infringed its images – third party web sites that copied, displayed and distributed unauthorized Perfect 10 images, individual users of Google’s search engine who stored full size Perfect 10 images on their computers, and users who linked to infringing web sites, thereby automatically making cache copies of full size images in their computers. Google did not dispute that third party web sites directly infringed Perfect 10’s copyrights by copying, displaying and distributing unauthorized copies of Perfect 10 images.⁶⁴⁹

The Ninth Circuit agreed, however, with the district court that Perfect 10 failed to provide any evidence directly establishing that users of Google’s search engine had stored infringing images on their computers. Finally, the Ninth Circuit agreed with the district court that any cache copies of full size images made by users who linked to infringing web sites were a fair use. The copying performed automatically by a user’s computer to assist in accessing the Internet was a transformative use and did not supersede the copyright holder’s exploitation of the work.⁶⁵⁰ “Such automatic background copying has no more than a minimal effect on Perfect 10’s rights, but a considerable public benefit.”⁶⁵¹ Accordingly, the Ninth Circuit assessed Google’s secondary liability based solely with respect to activities of third party web sites that reproduced, displayed, and distributed unauthorized copies of Perfect 10’s images on the Internet.⁶⁵²

Turning to whether Google could be secondarily liable for the infringing acts of those third party web sites, the Ninth Circuit first noted that under the Sony doctrine, Google could not be held liable for contributory infringement based solely on the fact that the design of its search engine facilitated such infringement. Nor, under footnote 12 of the Supreme Court’s Grokster decision, could Google be held liable solely because it did not develop technology that would enable its search engine to automatically avoid infringing images.⁶⁵³

The Ninth Circuit next held that Google could not be liable under the Supreme Court’s inducement test in Grokster, because Google had not promoted the use of its search engine

⁶⁴⁷ Id. at 855-56.

⁶⁴⁸ Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146 (9th Cir. 2007).

⁶⁴⁹ Id. at 1169.

⁶⁵⁰ Id.

⁶⁵¹ Id.

⁶⁵² Id. at 1170.

⁶⁵³ Id.

specifically to infringe copyrights.⁶⁵⁴ In reaching this result, however, the Ninth Circuit appears to have put a gloss on the Supreme Court's test for inducement liability, for in addition to noting that inducement liability could result from intentionally encouraging infringement through specific acts, the Ninth Circuit stated that intent could be imputed "if the actor knowingly takes steps that are substantially certain to result in ... direct infringement."⁶⁵⁵

Finally, turning to whether Google could have secondary liability under the traditional common law doctrine of contributory liability, the Ninth Circuit, citing its Napster decisions, noted that it had "further refined this test in the context of cyberspace to determine when contributory liability can be imposed on a provider of Internet access or services."⁶⁵⁶ The Ninth Circuit noted that under both Napster and Netcom, a service provider's knowing failure to prevent infringing actions could be the basis for imposing contributory liability, because under such circumstances, the intent required under the Supreme Court's Grokster decision may be imputed. Accordingly, the Ninth Circuit articulated the following test for contributory liability in the context of cyberspace:

[W]e hold that a computer system operator can be held contributorily liable if it "has *actual* knowledge that *specific* infringing material is available using its system," Napster, 239 F.3d at 1002, and can "take simple measures to prevent further damage" to copyrighted works, Netcom, 907 F. Supp. At 1375, yet continues to provide access to infringing works.⁶⁵⁷

This articulated test leaves open at least the following questions, with respect to which the Ninth Circuit's decision gives little guidance:

- Is this the exclusive test for contributory infringement in "the context of cyberspace"?
- What are the boundaries of "the context of cyberspace" within which this test will apply?
- Does the reference to "actual" knowledge preclude secondary liability on the alternative traditional common law formulation of "reason to know" in the context of cyberspace?
- Do "simple measures" extend only to taking down specific infringing material, or to preventing its recurrence also?

Applying this specialized test, the Ninth Circuit ruled that the district court had erred in concluding that, even if Google had actual knowledge of infringing material available on its

⁶⁵⁴ Id. at 1171 n.11.

⁶⁵⁵ Id. at 1171.

⁶⁵⁶ Id.

⁶⁵⁷ Id. at 1172 (emphasis in original).

system, it did not materially contribute to infringing conduct because it did not undertake any substantial promotional or advertising efforts to encourage visits to infringing web sites, nor provide a significant revenue stream to the infringing web sites.⁶⁵⁸ The Ninth Circuit stated:

There is no dispute that Google substantially assists websites to distribute their infringing copies to a worldwide market and assists a worldwide audience of users to access infringing materials. We cannot discount the effect of such a service on copyright owners, even though Google's assistance is available to all websites, not just infringing ones. Applying our test, Google could be held contributorily liable if it had knowledge that infringing Perfect 10 images were available using its search engine, could take simple measures to prevent further damage to Perfect 10's copyrighted works, and failed to take such steps.⁶⁵⁹

Noting that there were factual disputes over whether there are "reasonable and feasible means" for Google to refrain from providing access to infringing images, the Ninth Circuit remanded the contributory infringement claim for further consideration of whether Perfect 10 would likely succeed in establishing that Google was contributorily liable for inline linking to full size infringing images under the test the court had enunciated.⁶⁶⁰

Similarly, the Ninth Circuit remanded for further proceedings on whether Amazon.com, which Perfect 10 had also sued based on its offering of the A9.com search engine, should be held contributorily liable. "It is disputed whether the notices gave Amazon.com actual knowledge of specific infringing activities available using its system, and whether Amazon.com could have taken reasonable and feasible steps to refrain from providing access to such images, but failed to do so."⁶⁶¹

Vicarious Liability. Perfect 10 also asserted claims against Google for vicarious liability. With respect to the financial benefit prong, the district court found that Google obtained a direct financial benefit from the infringing activity through its AdSense revenues under the standard articulated in the Ninth Circuit's Fonovisa decision,⁶⁶² in which it held that the financial benefit prong can be satisfied where the availability of infringing material acts as a "draw" for customers to the site. Under that standard, the district court found it likely that at least some users were drawn to Google Image Search because they knew that copies of Perfect 10's photos could be viewed for free, and Google derived a direct financial benefit when users visited AdSense partners' web sites that contained such infringing photos.⁶⁶³

⁶⁵⁸ Id.

⁶⁵⁹ Id.

⁶⁶⁰ Id. at 1172-73

⁶⁶¹ Id. at 1176.

⁶⁶² Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996).

⁶⁶³ Perfect 10 v. Google, 416 F. Supp. 2d at 856-57.

Notwithstanding the financial benefit to Google, however, the district court found that Google had insufficient control over the infringing activity to impose vicarious liability because the Web is an open system. “Google does not exercise control over the environment in which it operates – i.e., the web. Google’s ability to remove a link from its search index does not render the linked-to site inaccessible. The site remains accessible both directly and indirectly (i.e., via other search engines, as well as via the mesh of websites that link to it). If the phrase ‘right and ability to control’ means having substantial input into or authority over the decision to serve or continue serving infringing content, Google lacks such right or ability.”⁶⁶⁴ Moreover, Google’s software lacked the ability to analyze every image on the Internet, compare each image to all other copyrighted images that existed in the world, or even to that much smaller subset of images that had been submitted to Google by copyright owners such as Perfect 10, and determine whether a certain image on the web infringed someone’s copyright.⁶⁶⁵ Finally, the court ruled that the “right and ability to control” prong required more than Google’s reservation in its AdSense policy of the right to monitor and terminate partnerships with entities that violated others’ copyrights. Accordingly, the district court held that Perfect 10 had not established a likelihood of proving the second prong necessary for vicarious liability.⁶⁶⁶

Based on its various rulings, the district court concluded that it would issue a preliminary injunction against Google prohibiting the display of thumbnails of Perfect 10’s images, and ordered the parties to propose jointly the language of such an injunction.⁶⁶⁷

On appeal, the Ninth Circuit affirmed the district court’s ruling that Perfect 10 had not shown a likelihood of establishing Google’s right and ability to stop or limit the directly infringing conduct of third party web sites. The Ninth Circuit began its analysis by noting that, under *Grokster*, “a defendant exercises control over a direct infringer when he has both a legal right to stop or limit the directly infringing conduct, as well as the practical ability to do so.”⁶⁶⁸ With respect to the first part of this test, the court noted that, unlike in *Fonovisa* where the swap meet operator had contracts with its vendors giving it the right to stop the vendors from selling counterfeit recordings on its premises, Perfect 10 had not shown that Google had contracts with third party web sites that empowered Google to stop or limit them from reproducing, displaying and distributing infringing copies of Perfect 10’s images. Although Google had AdSense agreements with various web sites, an infringing third party web site could continue to reproduce, display, and distribute its infringing copies after its participation in the AdSense program was ended.⁶⁶⁹ And unlike the Napster system, in which Napster’s control over its closed system that required user registration and enabled Napster to terminate its users’ accounts and block their access to the Napster system, Google could not terminate third party web sites

⁶⁶⁴ *Id.* at 857-58.

⁶⁶⁵ *Id.* at 858.

⁶⁶⁶ *Id.*

⁶⁶⁷ *Id.* at 859.

⁶⁶⁸ *Perfect 10 v. Amazon.com, Inc.*, 508 F.3d 1146, 1173 (9th Cir. 2007).

⁶⁶⁹ *Id.*

distributing infringing photographs or block their ability to host and serve infringing full size images on the Internet.⁶⁷⁰

The Ninth Circuit also affirmed the district court's findings that Google lacked the practical ability to police the third party web sites' infringing conduct. "Without image-recognition technology, Google lacks the practical ability to police the infringing activities of third-party websites."⁶⁷¹ Google's inability to police distinguished it from the defendants held liable in the Napster and Fonovisa cases. Accordingly, Perfect 10 had failed to establish the right and ability to control prong of vicarious liability.⁶⁷² Having so concluded, the Ninth Circuit determined that it need not reach Perfect 10's argument that Google received a direct financial benefit.⁶⁷³

Based on its rulings, the Ninth Circuit reversed the district court's determination that Google's thumbnail versions of Perfect 10's images likely constituted a direct infringement. It also reversed the district court's conclusion that Perfect 10 was unlikely to succeed on the merits of its secondary liability claims because the district court failed to consider whether Google and Amazon.com knew of infringing activities yet failed to take reasonable and feasible steps to refrain from providing access to infringing images. Accordingly, the Ninth Circuit remanded the case to the district court for further proceedings on this point, as well as to consider whether Google and Amazon.com would qualify for any of the safe harbors of the DMCA, an issue which the district court did not consider because of its rulings. Because the district court would need to reconsider the appropriate scope of injunctive relief after addressing the secondary liability issues, the Ninth Circuit decided that it need not address the parties' dispute over whether the district court abused its discretion in determining that Perfect 10 satisfied the irreparable harm element of a preliminary injunction.⁶⁷⁴

On remand, Google asserted various safe harbors under the DMCA. Analysis of the rulings with respect to whether Google was entitled to any of the safe harbors may be found in Section III.C.6(b)(1)(ii).c.

5. Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey

In Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey,⁶⁷⁵ the court ruled that display of copyrighted images on computer monitors within a law office constituted a public

⁶⁷⁰ Id. at 1174.

⁶⁷¹ Id.

⁶⁷² Id. The Ninth Circuit also stated, without analysis, that it agreed with the district court's conclusion that Amazon.com did not have the right and ability to supervise the infringing activity of Google or third parties, and that the district court did not clearly err in concluding that Amazon.com lacked a direct financial interest in such activities. Id. at 1176.

⁶⁷³ Id. at 1175 n.15.

⁶⁷⁴ Id. at 1176-77.

⁶⁷⁵ 2007 U.S. Dist. LEXIS 52544 (E.D. Pa. July 20, 2007).

display, but was permitted under the fair use doctrine. Healthcare Advocates had filed a lawsuit alleging that a competitor infringed trademarks and copyrights and misappropriated trade secrets belonging to Healthcare Advocates. The defendants in that case were represented by the boutique IP law firm of Harding, Earley, Follmer & Frailey. To aid in preparing a defense, on two occasions employees of the Harding firm accessed screenshots of old versions of Healthcare Advocates' web sites that had been archived by the Internet Archive's web site (www.archive.org). The old versions of the web site were accessed through the "Wayback Machine," an information retrieval system offered to the public by the Internet Archive that allowed users to request archived screenshots contained in its archival database. Viewing the content that Healthcare Advocates had included on its public web site in the past was very useful to the Harding firm in assessing the merits of the trademark and trade secret allegations brought against the firm's clients. The Harding firm printed copies of the archived screenshots of interest and used the images in the litigation against their clients. Healthcare Advocates then sued the Harding firm, alleging that viewing the screenshots of the old versions of their web site on computers within the firm constituted an infringing public display, and that printing of copies of those screenshots and storing them on hard drives at the firm also infringed the company's copyrights.⁶⁷⁶

The court ruled that, "[u]nder the expansive definition of a public display, the display of copyrighted images on computers in an office constitutes a public display."⁶⁷⁷ The court concluded, however, that the Harding firm's display and copying of those images for purposes of defending its clients in the litigation brought by Healthcare Associates constituted a fair use. With respect to the purpose of the use, the court noted that the images were used to better understand what Healthcare Associates' complaint, which did not specify what had been infringed nor have any documents attached to it depicting the infringement, was based on.⁶⁷⁸ Only a small group of employees were able to see the images within the law firm's office, which the court found was "similar to a family circle and its acquaintances."⁶⁷⁹ The purpose of the printing was only to make a record of what had been viewed and for use as supporting documentation for the defense the firm planned to make for its clients.⁶⁸⁰ "It would be an absurd result if an attorney defending a client against charges of trademark and copyright infringement was not allowed to view and copy publicly available material, especially material that his client was alleged to have infringed."⁶⁸¹

The second fair use factor weighed in favor of the firm because the nature of Healthcare Associates' web sites was predominantly informational. The third factor weighed in favor of the

⁶⁷⁶ Id. at *2-10.

⁶⁷⁷ Id. at *19.

⁶⁷⁸ Id. at *22-23.

⁶⁷⁹ Id. at *24. The copyright statute defines a "public" display as one made in a place "where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered." 17 U.S.C. § 101.

⁶⁸⁰ Id. at *24.

⁶⁸¹ Id. at *24-25.

firm because, although entire images were copied, employees at the firm needed to copy everything they viewed because they were using the screenshots to defend their clients against copyright and trademark infringement claims. The firm also had a duty to preserve relevant evidence. Finally, the court found that the fourth fair use factor also favored the firm, because the value of Healthcare Associates' web sites was not affected by the Harding's firm's use, and the images viewed and copied were archived versions of the web site that Healthcare Associates no longer utilized, suggesting their worth was negligible. Accordingly, the court held that the Harding firm's use of the images obtained through the Wayback Machine constituted a fair use.⁶⁸²

6. ICG-Internet Commerce Group, Inc. v. Wolf

In ICG-Internet Commerce Group, Inc. v. Wolf,⁶⁸³ the court held that the defendant had infringed the plaintiff's copy and public display rights in an adult video by posting the video to the defendant's web site. The court also ruled that the insertion into the plaintiff's video of a URL link to the defendant's web site constituted the creation of an infringing derivative work.⁶⁸⁴

7. Perfect 10 v. Yandex

In Perfect 10, Inc. v. Yandex, N.V.,⁶⁸⁵ Yandex operated image search engines at Yandex.ru, whose servers were located in Russia, and Yandex.com, whose servers were located in the U.S. Yandex.ru was Russia's most popular search engine and the fourth largest search engine worldwide. The search engines did not store any full-sized images that its crawlers located, but rather stored only lower-resolution thumbnails of the images. Yandex reproduced its thumbnail copies on search results pages so that a user making a search query could determine which, if any, thumbnails were of interest and then click through to the third party web site that hosted the full-sized image. When the user clicked on a link, the full-size source image was displayed via inline linking in the same browser window without including other parts of the surrounding third-party web page on which the full-sized image appeared. Thumbnails of several thousand unauthorized Perfect 10 images were stored on Yandex's search engine servers and Perfect 10 sued for direct, contributory and vicarious copyright infringement. Yandex moved for summary judgment on several issues.⁶⁸⁶

Turning first to the issue of direct liability, the court noted that of the 63,756 alleged infringements to which Yandex.ru and Yandex.com linked in search results, 51,959 of them were

⁶⁸² Id. at *26-29. The court also ruled that the firm's failure to preserve temporary cache files of the screenshots that were automatically created by the computers used by the firm's employees to view the images through the Internet, and were also automatically deleted by the computers' operating system, did not constitute spoliation of evidence. Id. at *30-38.

⁶⁸³ 519 F. Supp. 2d 1014 (E.D. Pa. 2007).

⁶⁸⁴ Id. at 1018.

⁶⁸⁵ 962 F. Supp. 2d 1146 (N.D. Cal. 2013).

⁶⁸⁶ Id. at 1150-51, 1155.

hosted on servers located outside the U.S. The court noted that under the Ninth Circuit’s “server test” adopted in the Perfect 10 v. Amazon case, the hosting web site’s computer, rather than the search engine’s computer, is the situs of direct infringement, and Yandex could therefore have no liability for direct infringement under U.S. copyright law with respect to those images hosted outside the U.S. The court rejected Perfect 10’s argument that Yandex committed direct infringement by display in the U.S. of images hosted outside the U.S. because users in the U.S. could download them. Nowhere in the Amazon decision did the Ninth Circuit endorse the idea that display of a copyrighted image anywhere in the world creates direct copyright liability in the U.S. merely because images could be downloaded from a server abroad by someone in the U.S. The court observed that such a principle would destroy the concept of territoriality inhering in the Copyright Act for works on the Internet. The court found more plausible Perfect 10’s argument that, when Yandex’s servers were located in the U.S. for a nine-month period, a Yandex.com image search performed by a server in the U.S. could have linked to a Perfect 10 image hosted on a Yandex server in Russia. The court, however, found it unnecessary to address the validity of the argument because Perfect 10 had not demonstrated that Yandex in fact stored or displayed full-sized copies of the Perfect 10 images on Yandex’s U.S. servers. Accordingly, the court granted Yandex summary judgment on direct infringement with respect to hosting or display of Perfect 10 images through servers outside the U.S.⁶⁸⁷

The court then turned to storage of thumbnail versions of Perfect 10 images on Yandex.com servers in the U.S. during the nine-month period from June 2012 to March 2013. Yandex did not dispute that its use of the thumbnails in the U.S. constituted a prima facie violation of Perfect 10’s display and distribution rights, but argued that its thumbnail copies were a fair use. The court agreed. With respect to the first fair use factor, citing the Amazon and Kelly v. Arriba cases, the court found that use of a thumbnail image as a pointer to a source of information is highly transformative, and noted that Yandex’s in-linking to a full-size image, which caused it to be transmitted from the third party web site hosting it, did not constitute direct infringement on the part of Yandex.⁶⁸⁸

The court noted that the second fair use factor slightly favored the plaintiff Perfect 10, as in Amazon. With respect to the third factor, the amount and substantiality of the use, the court rejected Perfect 10’s argument that the third factor should favor it because Yandex allegedly used 40,000 Perfect 10 thumbnails. The court noted that the substantiality analysis must be made on a copyright-by-copyright basis, and the number of allegedly infringed images is therefore not relevant. As in Amazon and Kelly, the court concluded that the third factor favored neither party because Yandex’s transformative use required use of the entire image, although in reduced size. With respect to the fourth factor, the court rejected Perfect 10’s argument that Yandex’s search engines caused it market harm because they led to billions of unauthorized views and downloads of its images from web sites to which Yandex linked Perfect 10 thumbnails. The court found that Perfect 10 had not substantiated the argument by competent evidence. Perfect 10’s evidence consisted of screen shots from third party web sites

⁶⁸⁷ Id. at 1153-54.

⁶⁸⁸ Id. at 1154-55.

showing that links on those sites leading to Perfect 10 images had been viewed approximately 3.8 million times, but Perfect 10 failed to provide evidence that any of those views were the result of Yandex.com users clicking on thumbnails stored on Yandex.com servers in the U.S. during the nine-month period. The court also rejected Perfect 10's argument that its market for reduced-size images for cell phone use had dried up since 2007 and Yandex had begun providing a thumbnail search service since 2007; ergo, Perfect 10 had been harmed by Yandex. The court noted that this simple correlation, without more, did not constitute sufficient evidence that Yandex's use of 40,000 thumbnail images during the nine-month period affected Perfect 10's market for reduced-size images. The court therefore concluded that the fourth factor favored neither party. Balancing the four factors, the court ruled that Yandex.com's thumbnails stored on its servers in the U.S. for the nine-month period were fair use.⁶⁸⁹

Finally, the court ruled that Yandex could have potential contributory and vicarious liability only with respect to direct infringements taking place in the U.S., which eliminated contributory or vicarious liability for links connecting to full-size images hosted outside the U.S. The court therefore granted summary judgment to Yandex to that extent. The court then ruled that the case would proceed to trial with respect to liability pertaining to evidence submitted by Perfect 10 of 23 links that connected to U.S. web sites.⁶⁹⁰

8. Leader's Inst. v. Jackson

In this case, the defendant Magnovo Training Group (Magnovo) asserted a counterclaim that the plaintiff, The Leadership Institute (TLI), committed copyright infringement by framing Magnovo's copyrighted content. It was undisputed that when a user visited one of TLI's web sites, TLI's web site instructed the user's browser to display Magnovo's web site under TLI's web address. TLI sought summary judgment on the counterclaim, asserting that framing is not copyright infringement. The court rejected TLI's argument. TLI had displayed those works by "show[ing] a copy" of the works via a "process," as required by the definition of "display" in Section 101. The "process" was the instructing of users' web browsers to display Magnovo's copyrighted works when those users visited one of the accused TLI domain names. And TLI displayed the copyrighted work publicly – by instructing users' web browsers to display Magnovo's content upon accessing TLI's publicly-accessible web sites, TLI "transmit[ed] ... a display of [Magnovo's] work ... to the public" as required by the definition of a public display in Section 101. Thus, by framing Magnovo's copyrighted works, TLI impermissibly displayed the works to the public.⁶⁹¹

The court rejected TLI's reliance on the Ninth Circuit's decision in Perfect 10 v. Amazon, discussed in Section II.C.4 above. First, the court distinguished the facts of the present case from Perfect 10 v. Amazon, in which Google did not actually display infringing images but instead provided links for users to access sites that displayed infringing images. Although the infringing

⁶⁸⁹ Id. at 1156-57.

⁶⁹⁰ Id. at 1157-58 & n.3.

⁶⁹¹ Leader's Inst., LLC v. Jackson, 2017 U.S. Dist. LEXIS 193555 at *30-35 (N.D. Tex. Nov. 22, 2017).

content appeared under a Google banner, the user was essentially navigating to an infringing web site to view Perfect 10's photos. The same was not true of users who visited the accused TLI web sites. Upon visiting one of the TLI sites, a user would necessarily see Magnovo's content. Unlike Google, TLI did not merely provide a link by which users could access Magnovo content but instead displayed Magnovo's content as if it were its own.⁶⁹²

Second, the court rejected the Ninth Circuit's "server test," to the extent it makes actual possession of a copy a necessary condition to violating a copyright owner's public display right. The court noted that the text of the Copyright Act does not make actual possession of a copy of a work a prerequisite for infringement. Under Section 101, to display a work, a person need only show a copy of the work and need not actually possess a copy to display a work. And to display a work publicly, a person need only transmit or communicate a display to the public, and need not possess the display. For example, the court reasoned, a person that went into a movie theater and used a video camera connected to the Internet to broadcast a movie to the public would clearly be committing copyright infringement even though the person did not herself have a copy of the movie. Essentially then, the court viewed TLI's framing scheme as like a live feed of Magnovo's copyrighted web site. Whatever a user would see if she accessed Magnovo's web site, she would see if she accessed one of the accused TLI web sites. The court therefore concluded that, because Magnovo did not have to show that TLI had a copy of Magnovo's works, Magnovo's copyright infringement claim did not fail as a matter of law, and the court denied TLI's motion for summary judgment on the merits of Magnovo's copyright infringement counterclaim.⁶⁹³

9. Goldman v. Breitbart News Network

In Goldman v. Breitbart News Network, LLC,⁶⁹⁴ the court disagreed with the "server test" adopted by the Ninth Circuit in Perfect 10 v. Amazon (discussed in Section II.C.4 above), in addition to distinguishing it factually. In this case, the plaintiff's copyrighted photo of Tom Brady went viral from Snapchat to Reddit to Twitter, eventually making its way onto the web sites of the defendants in a Tweet that the defendants embedded alongside articles they wrote about Tom Brady actively helping the Boston Celtics recruit basketball player Kevin Durant. The plaintiff sued the defendants for violation of his display right.⁶⁹⁵

None of the defendants' web sites copied and saved the photo onto their own servers. Rather, they made the photo visible in their articles through a technical process known as "embedding." The court explained that "embedding" an image on a web page is the act of a coder intentionally adding a specific "embed" code to the HTML instructions for the page that incorporates an image hosted on a third party server onto the page. The embed code directs a

⁶⁹² Id. at *30-31.

⁶⁹³ Id. at *32-35.

⁶⁹⁴ 302 F. Supp. 3d 585 (S.D.N.Y. 2018).

⁶⁹⁵ Id. at 586.

browser to the third party server via a hyperlink to retrieve the image. Here, it was undisputed that none of the defendants' web sites actually downloaded the photo from Twitter, copied it, and stored it on their own servers. Rather, each of defendants' web sites merely embedded the photo by including the necessary embed code in their HTML instructions. As a result, all of the defendants' web sites included articles about the meeting between Tom Brady and the Celtics, with the full size photo visible without the user having to click on a hyperlink, or a thumbnail, in order to view the photo.⁶⁹⁶

The defendants urged the court to adopt the Ninth Circuit's server test to define the scope of the display right. The district court began its analysis with a survey of existing case law discussing the server test. It noted that only four courts in the S.D.N.Y. had discussed the server test and Perfect 10's holding, but none had adopted it for the display right. The court further noted that, although the Seventh Circuit had adopted the server test for contributory liability in Flava Works v. Gunter (discussed in Section III.C.2(m) below), in the only decision to consider the server test in relation to the display right, The Leader's Inst., LLC v. Jackson (discussed in Section II.C.8 above), the court ruled that the plaintiffs infringed the defendant's exclusive display right by framing the defendant's web sites, distinguishing Perfect 10 on its facts.⁶⁹⁷

The court rejected the server test as improper for determining the scope of the display right, finding that the plain language of the Copyright Act and its legislative history provided no basis for a rule that allows the physical location or possession of an image to determine who may or may not have "displayed" a work within the meaning of the Copyright Act. The court noted that nowhere does the Copyright Act suggest that possession of an image is necessary in order to display it, and the purpose and language of the Act support the opposite view. Section 101 defines the display of a work publicly to include the transmission of a display of the work by means of any device or process. To transmit a display is similarly defined as the communication of it by any device or process whereby images or sounds are received beyond the place from which they are sent. Devices and processes are further defined to include ones now known or later developed. The court observed that these definitions were plainly drafted with the intent to sweep broadly.⁶⁹⁸

Here, the defendants' web sites actively took steps to display the plaintiff's photo by embedding a code in the web sites' HTML that resulted in a transmission of the photo so that it could be visibly shown. The court stated that, properly understood, the steps necessary to embed a Tweet were accomplished by the defendants' web sites, and those steps constituted a "process." The plain language of the Copyright Act calls for no more.⁶⁹⁹ The court also pointed to legislative history stating that the Act was intended to include "each and every method by which images ... comprising a ... display are picked up and conveyed" and that an infringement of

⁶⁹⁶ Id. at 587.

⁶⁹⁷ Id. at 590-92.

⁶⁹⁸ Id. at 593.

⁶⁹⁹ Id. at 593-94.

the display right could occur “if the image were transmitted by any method (... for example, by a computer system) from one place to members of the public elsewhere.”⁷⁰⁰ The court therefore concluded that nothing in either the text or purpose of the Copyright Act suggested that physical possession of an image is a necessary element to its display for purposes of the Act.⁷⁰¹ The court also found indirect support for its rejection of the server test in “the principles that undergird the [Supreme Court’s] Aereo decision – chief among them that mere technical distinctions invisible to the user should not be the lynchpin on which copyright liability lies.”⁷⁰²

The court declined to adopt the server test of Perfect 10 on the further ground that, by focusing on making a “copy” for storage on the server of the image to be displayed, the test erroneously collapses the display right into the reproduction right. The court found this inconsistent with several distinct parts of the Copyright Act that contemplate infringers who would not be in possession of copies – for example, in Section 110(5)(A), which exempts small commercial establishments whose proprietors merely bring onto their premises standard radio or television equipment and turn it on for their customer’s enjoyment, even though the proprietors are not making any copies.⁷⁰³

In addition, the court noted that, even if the Perfect 10 decision correctly interpreted the Act, the court disagreed with the defendants that Perfect 10 stands for a broadly construed server test that focuses solely on the physical location of allegedly infringing images. The court noted that Perfect 10 was heavily informed by two factors – the fact that the defendant operated a search engine, and the fact that the user made an active choice to click on an image before it was displayed – which suggest that a broad reading of it is neither appropriate nor desirable. The court distinguished the present case factually on those two factors. In Perfect 10, Google’s search engine provided a service whereby the user navigated from web page to web page, with Google’s assistance. Such navigation was manifestly not the same as opening up a favorite blog or web site to find a full color image awaiting the user, whether he or she asked for it, looked for it, clicked on it, or not. In the court’s view, both the nature of Google’s search engine, as compared to the defendants’ web sites, and the volitional act taken by users of Google’s services, provided a sharp contrast to the facts in this case. Accordingly, the court refused to apply the server test as neither appropriate to the specific facts of this case nor adequately grounded in the text of the Copyright Act. The court therefore denied the defendants’ motion for partial summary judgment on that basis.⁷⁰⁴

⁷⁰⁰ Id. at 594 (quoting H.R. Rep. 94-1476, 64, 70 (1976)).

⁷⁰¹ Breitbart News, 302 F. Supp. 3d at 594.

⁷⁰² Id. at 594-95.

⁷⁰³ Id. at 595.

⁷⁰⁴ Id. at 595-96.

10. Nicklen v. Sinclair Broad. Grp.

In this case, the plaintiff captured footage of a starving polar bear and posted the video to his Instagram and Facebook accounts. Dozens of news outlets and online publishers, including the defendants, embedded the video in online articles via inlinks without a license. The plaintiff sued for violation of his public display right. The defendants moved to dismiss based on the server test and fair use.⁷⁰⁵

The court ruled that embedding a video displays the video within the meaning of the Copyright Act, finding that under the plain meaning of the definition of “display,” a defendant violates an author’s exclusive right to display an audiovisual work publicly when the defendant without authorization causes a copy – not the first copy, or the only copy, but any copy – of the work, or individual images of the work, to be seen, whether directly or by means of any device or process known at the time of the passage of the Copyright Act of 1976 or thereafter. The court noted that the exclusive display right in the copyright statute is technology-neutral and is therefore concerned not with how a work is shown, but that at work is shown. Embedding a video on a web site displays that video, because to embed a video is to show the video or individual images of the video non-sequentially by means of a device or process. The court therefore viewed the embed code on the defendants’ web pages as simply an information retrieval system that permitted the plaintiff’s video or an individual of the video to be seen. The defendants’ act of embedding therefore fell squarely within the display right.⁷⁰⁶

The court refused to adopt the Ninth Circuit’s server test, finding it contrary to the text and legislative history of the copyright statute. The statute defines to display as “to show a copy of” a work, not “to make and then show a copy of the copyrighted work.” The court found that the Ninth Circuit’s approach, under which no display is possible unless the alleged infringer has also stored a copy of the work on the infringer’s computer, therefore makes the display right merely a subset of the reproduction right. The court also believed that the Ninth Circuit’s reasoning in the Perfect 10 case should be cabined by two facts specific to that case: (1) the defendant operated a search engine and (2) the copyrighted images were displayed only if a user clicked on a link in order to see the full image rather than merely the thumbnail that Google’s search engine had displayed. In the instant case, an individual still image from the plaintiff’s video awaited the defendants’ readers whether they clicked the image to play the video or not. The court therefore concluded that the Perfect 10 test was a poor fit for the instant case and declined to adopt it.⁷⁰⁷

The court also noted practical problems with the server test. Under that test, a photographer who promotes his work on Instagram or a filmmaker who posts her short film on YouTube surrenders control over how, when, and by whom their work is subsequently shown –

⁷⁰⁵ Nicklen v. Sinclair Broad. Grp., 2021 U.S. Dist. LEXIS 142768 at *3-4 (S.D.N.Y. July 30, 2021).

⁷⁰⁶ Id. at *9-12.

⁷⁰⁷ Id. at *12-15.

reducing the display right, effectively, to the limited right of first publication that the Copyright Act of 1976 rejects.⁷⁰⁸

The court next ruled that the defendants had not met their difficult burden of proving a fair use defense on the pleadings. Under the first factor, the court noted that the use was commercial, but might also be transformative. For example, a news report about a video that had gone viral on the Internet might fairly display a screenshot or clip from that video to illustrate what all the fuss was about, thereby transforming the function of the work in the new context. The first factor therefore weighed in favor of fair use. The second factor neither weighed strongly for or against fair use. Although the video expressed creativity in its making, it also purported to depict reality and could therefore be viewed as news gathering.⁷⁰⁹

The third factor weighed against fair use because the defendants embedded the entire video on their web sites. A single image of the emaciated bear rather than an embedded copy of the full work could have conveyed that the video was shocking or heart-wrenching enough to grab the attention of Internet users. The fourth factor also weighed against fair use. The court first observed that because a news article recontextualizes a work and serves a different purpose, it is unlikely that someone who wanted to purchase the work would find reviewing the news article an adequate substitute. However, the defendants' use of the copyrighted video, if widespread, would harm the licensing market for the plaintiff's video. There would be no need for news outlets to license the video at all if each outlet could, without the plaintiff's prior authorization, embed the video from Instagram or Facebook. In sum, the court noted the fact intensive nature of the fair use factors and concluded that its fair use analysis would benefit from a better-developed factual record. The court therefore denied the defendants' motion to dismiss on grounds of fair use.⁷¹⁰

11. The "Server Test" Versus the "Incorporation Test"

An issue that has generated controversy in the courts is how "display" should be defined in the context of inline linking. Under the so-called "server test," display is defined as the act of *serving* content over the web, i.e., physically sending bits over the Internet to the user's browser. Under the server test, the entity that is deemed liable for the display of infringing content is the entity whose server served up the infringing material. Under the so-called "incorporation test," display is defined as the mere act of incorporating content into a web page that is then pulled up by the browser through an inline link. Under the incorporation test, the entity that is deemed liable for the display of infringing content is the entity that uses an inline link in its web page to direct the user's browser to retrieve the infringing content.

⁷⁰⁸ Id. at *15.

⁷⁰⁹ Id. at *16-19.

⁷¹⁰ Id. at *20-23.

The courts have split on which test to adopt for purposes of infringement of the display right.⁷¹¹

(a) Cases Accepting or Applying the Server Test

(1) Perfect 10 v. Google

This case, discussed in more detail in Section II.C.4 above, was the first case to formally adopt the server test. As discussed in more detail above, the Ninth Circuit agreed with the district court that the server test should be used to determine which entity displays an image on the web, concluding that the test was consistent with the statutory language of the copyright statute. The Ninth Circuit affirmed that Google's image search engine had not publicly displayed a copy of the full size infringing images when it framed inline linked images that appeared on a user's computer screen.⁷¹² The court found that Google's activities with respect to the full size images did not meet the statutory definition of public display "because Google transmits or communicates only an address which directs a user's browser to the location where a copy of the full-size image is displayed. Google does not communicate a display of the work itself."⁷¹³

(2) Perfect 10 v. Yandex

In this case, discussed in more detail in Section II.C.7 above, the defendant's search engine stored only lower-resolution thumbnails of images and reproduced those thumbnail images on search results pages. The user then clicked on thumbnail links of interest to display the full-size source image via inline linking. A district court in the N.D. Cal. applied the server test and granted summary judgment to the defendant because the plaintiff had not shown that any full sized images were stored on the defendant's servers in the U.S., and the defendant could not be liable for display in the U.S. of images that were stored on its server in Russia under the principle of territoriality in copyright law.⁷¹⁴

(3) Louis Vuitton v. Akanoc Solutions

In this case, discussed in more detail in Section III.C.1(a) below, a district court in the N.D. Cal. applied the server test to deny the defendants' motion for JMOL on the plaintiff's claim under the display right because the evidence established that the defendants' servers in China stored and served data, including pictures of the plaintiff's copyrighted merchandise, for sale to

⁷¹¹ The Seventh Circuit, in a confusing opinion by Judge Posner, appears to have adopted something akin to the server test for purposes of contributory liability in Flava Works v. Gunter, 689 F.3d 754 (7th Cir. 2012) (discussed in Section III.C.2(m) below).

⁷¹² Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1159-60 (9th Cir. 2007).

⁷¹³ Id. at 1161 n.7.

⁷¹⁴ Perfect 10 v. Yandex, 962 F. Supp. 2d 1146, 1150-51, 1153-55 (N.D. Cal. 2013).

U.S. customers, which was sufficient for direct infringement of the display right.⁷¹⁵ This decision seems inconsistent with the court’s decision in Perfect 10 v. Yandex with respect to application of the principle of territoriality.

(4) Hunley v. Instagram

The plaintiffs sued Instagram for violation of their public display rights on the ground that Instagram’s “embedding tool” enabled third party websites to display their copyrighted photos posted to an Instagram account. The court rejected the plaintiffs’ argument that the Perfect 10 server test should not apply to third party websites that embed images and videos shared on social media because Perfect 10 addressed a “search engine” and reflected a highly fact-driven policy judgment. The court found that, to the contrary, Perfect 10 relied on the plain language of the statute, not policy considerations, nor did Perfect 10 suggest that its holding was limited to the unique facts presented there. The court also rejected the plaintiffs’ argument that the Supreme Court’s Aereo decision was irreconcilable with Perfect 10’s reasoning. In Aereo, the Supreme Court was addressing the public performance right, not the public display right, which is embodied in different statutory language. Although the Aereo court found some ambiguity in the public performance right statutory language, it resolved that ambiguity by relying on legislative purposes unique to the performance right. The court therefore concluded that it was bound to follow Perfect 10’s server test as articulated by the Ninth Circuit and granted Instagram’s motion to dismiss.⁷¹⁶

(b) Cases Rejecting the Server Test, Distinguishing It, or Refusing to Adjudicate It

(1) Leader’s Institute v. Jackson

In this case, discussed in more detail in Section II.C.8 above, a district court in the N.D. Tex. rejected the Ninth Circuit’s server test to the extent it makes actual possession of a copy a necessary condition to violating a copyright owner’s public display right, noting that the text of the Copyright Act does not make actual possession of a copy of a work a prerequisite for infringement. The court also distinguished the facts of the Perfect 10 v. Google case on the ground that in that case Google did not actually display infringing images but instead provided links for users to access sites that displayed infringing images. The same was not true of users

⁷¹⁵ Louis Vuitton v. Akanoc Solutions, 2010 U.S. Dist. LEXIS 85266 at *11-15 (N.D. Cal. Mar. 19, 2010), aff’d in part & rev’d in part on other grounds, 658 F.3d 936 (9th Cir. 2011).

⁷¹⁶ Hunley v. Instagram, LLC, 2021 U.S. Dist. LEXIS 177667 at *3-7 (N.D. Cal. Sept. 17, 2021). The court noted that, to the extent another court in the N.D. Cal. had suggested (in dicta) that Perfect 10 applies only in the context of search engines, Free Speech Sys. V. Menzel, 390 F. Supp. 3d 1162, 1172 (N.D. Cal. 2019), the court disagreed with that ruling. Hunley, 2021 U.S. Dist. LEXIS 177667 at *5 n.1. The plaintiffs then filed an amended complaint alleging that third parties committed copyright infringement and that Instagram was secondarily liable for that infringement. The court dismissed the amended complaint without leave to amend, ruling that, although it included additional pages of text, most of it consisted of arguments that Perfect 10 was wrongly decided. The court found that, to the extent the amended complaint included revised factual allegations, they only confirmed that, under Perfect 10, the claims failed as a matter of law. Hunley v. Instagram, LLC, 2022 U.S. Dist. LEXIS 18036 at *3-4 (N.D. Cal. Feb. 1, 2022).

who visited the counter-defendant's web sites, at which they would necessarily see the infringing content via inline links.⁷¹⁷

(2) Goldman v. Breitbart News Network

In this case, discussed in more detail in Section II.C.9 above, a district court in the S.D.N.Y. disagreed with the server test, ruling that the plain language of the Copyright Act and its legislative history provide no basis for a rule that allows the physical location or possession of an image to determine who may or may not have "displayed" a work within the meaning of the Copyright Act. The court declined to adopt the server test on the further ground that, by focusing on making a "copy" for storage on the server of the image to be displayed, the test erroneously collapses the display right into the reproduction right.⁷¹⁸

The court also distinguished the Perfect 10 v. Google case on the basis that it was heavily informed by two factors not present in the instant case – the fact that the defendant operated a search engine, and the fact that the user made an active choice to click on an image before it was displayed.⁷¹⁹

(3) Free Speech Sys. v. Menzel

In this case the plaintiff brought a declaratory judgment action for a declaration that it had not directly, contributorily, or vicariously infringed the defendant's copyright. The defendant brought counterclaims for copyright infringement and violation of the DMCA's CMI removal provisions. The defendant alleged that the plaintiff posted without authorization on its InfoWars web site some of the defendant's photographs. When a reader clicked on the images of the photographs appearing on the InfoWars web site, the reader was taken to another web site, naturalsociety.com, where the images were stored. Among other claims, the defendant alleged that the plaintiff directly infringed the public display right. The plaintiff argued that under the Ninth Circuit's server test in Perfect 10 v. Google, it could not be liable for violation of the public display right because the images were not stored on its web site.⁷²⁰

Although the district court was sitting within the Ninth Circuit's jurisdiction, the court noted two problems with the plaintiff's wholesale reliance on Perfect 10. First, the plaintiff cited no case applying the Perfect 10 server test outside of the context of search engines, and noted that subsequent cases had refused to apply the server test outside of that context.⁷²¹ While noting that those cases were from outside the Ninth Circuit, the court also noted that the defendant had not provided any case within the Ninth Circuit applying the server test outside of

⁷¹⁷ Leader's Inst. v. Jackson, 2017 U.S. Dist. LEXIS 193555 at *27-30 (N.D. Tex. Nov. 22, 2017).

⁷¹⁸ Goldman v. Breitbart News Network, 302 F. Supp. 3d 585, 593, & 595 (S.D.N.Y. 2018).

⁷¹⁹ Id. at 595-96.

⁷²⁰ Free Speech Sys. v. Menzel, 390 F. Supp. 3d 1162, 1167 & n.2, 1171 (N.D. Cal. 2019).

⁷²¹ Id. at 1172, citing the Goldman v. Breitbart News and Leader's Institute v. Jackson cases discussed in subsections (1) and (2) above.

the search engine context or in the context of the present case (involving the wholesale posting of copyrighted material on a news site). Second, even if the server test applied, the court was not willing at the early stage of the case to take judicial notice that the defendant's photographs were hosted only on the naturalsociety.com web site and were never saved on InfoWars' servers. Accordingly, the court ruled that the defendant's counterclaim for direct infringement of the public display right had been adequately alleged and denied the plaintiff's motion to dismiss that claim.⁷²²

(4) Sinclair v. Ziff Davis

The plaintiff sued Mashable, Inc. and its parent company, Ziff Davis, LLC, alleging that they infringed the plaintiff's copyright when Mashable posted on its web site a photograph that the plaintiff had posted on her Instagram site. The photograph was embedded within an article on the Mashable site. Mashable used "embed codes" within the article that caused a reader's browser to retrieve the embedded photograph from the Instagram server and display it on Mashable's web site. Instagram made available an application programming interface (API) that enabled users to access and share, via embed codes, content posted by other users whose accounts were set to "public" mode. The court noted that Instagram's Terms of Use (TOU) for its site stated that, by posting content to Instagram, the user "grant[s] to Instagram a non-exclusive, fully paid and royalty-free, transferable, sub-licensable, worldwide license to the Content that you post on or through [Instagram], subject to [Instagram's] Privacy Policy." The TOU further stated that content users uploaded and designated as "public" was searchable by the public and subject to use by others via Instagram's API. The court therefore initially ruled that, because the plaintiff had uploaded her photograph to Instagram and designated it as "public," she agreed to allow Mashable, as Instagram's sublicensee, to embed the photograph in its web site through Instagram's API.⁷²³

In a footnote, the court stated that, because it had found that Instagram granted Mashable a valid license to display the photograph, it need not reach the question, unsettled in the Second Circuit at that time, of whether embedding an image constitutes a "display" that is capable of infringing a copyright in the image.⁷²⁴

In a subsequent opinion issued a couple of months later upon a motion for reconsideration, the court revised its initial ruling. The court adhered to its previous holding that, by agreeing to Instagram's TOU, the plaintiff authorized Instagram to grant API users, such

⁷²² Menzel, 390 F. Supp. 3d at 1172. The court did, however, dismiss the defendant's counterclaim for removal of CMI for inadequate factual pleading. With respect to the defendant's Section 1202(b)(1) claim, he had merely alleged that his photographs were altered to remove certain of his CMI without providing any facts to identify which photographs had CMI removed or to describe what the removed or altered CMI was. With respect to his Section 1202(b)(2) claim, he had not identified what CMI was allegedly distributed or how that was distributed, and without identifying what CMI was removed prior to distribution and how that distribution was accomplished by the plaintiffs. Id. at 1175.

⁷²³ Sinclair v. Ziff Davis, LLC, 454 F. Supp. 3d 342, 343-345 (S.D.N.Y. 2020).

⁷²⁴ Id. at 346 n.3.

as Mashable, a sublicense to embed her public Instagram content. The court, however, revised the earlier ruling by finding that the pleadings contained insufficient evidence that Instagram exercised its right to grant a sublicense to Mashable. As evidence of the purported sublicense, Mashable presented Instagram’s Platform Policy, which stated that Instagram “provide[s] the Instagram APIs to help broadcasters and publishers discover content, get digital rights to media, and share media using web embeds. The court found that in reaching its previous conclusion that this provision of the Platform Policy granted Mashable a sublicense to use the API to embed the photograph in its web site, the court did not give full effect to the legal requirement that a license must convey the licensor’s explicit consent to use a copyrighted work. The Platform Policy’s statement that the API was intended to help broadcasters and publishers discover content, get digital rights to media, and share media using web embeds could be interpreted to grant API users the right to use the API to embed the public content of other Instagram users. But the court found that is not the only interpretation to which that term is susceptible, citing the McGucken decision discussed in the next subsection. Accordingly, the court ruled that the Platform Policy’s terms were insufficiently clear to warrant dismissal of the plaintiff’s claims at the present stage of the litigation.⁷²⁵ In February of 2021, Mashable reached a settlement with the plaintiff.⁷²⁶

(5) McGucken v. Newsweek

The facts of this case were very similar to those of the Sinclair case discussed in the previous subsection. The defendant Newsweek published an article about an ephemeral lake and used an embed code to a photograph of the lake owned by the plaintiff that he had posted to his Instagram account. Newsweek moved to dismiss the action for failure to state a claim on the basis that, under Instagram’s Platform Policy (discussed in the summary of the Sinclair case in the previous subsection), it had a valid sublicense to use the photograph as a result of the plaintiff’s public post on Instagram or that Newsweek’s embedding was a fair use.⁷²⁷

The court rejected the motion to dismiss on the grounds of a sublicense, noting that Instagram’s Platform Policy instructed users to “[c]omply with any requirements or restrictions imposed of usage of Instagram photos and videos ... by their respective owners,” and also prohibited users from “provid[ing] or promot[ing] content that violates any rights of any person, including but not limited to intellectual property rights.” The court agreed that Instagram’s Terms of Use unequivocally granted Instagram a license to sublicense the plaintiff’s publicly posted content, but found there was no evidence before the court that Instagram had granted a

⁷²⁵ Sinclair v. Ziff Davis, LLC, 2020 U.S. Dist. LEXIS 110627 at *2-3 (June 24, 2020). In June of 2020, an Instagram spokesperson told Ars Technica: “While our terms allow us to grant a sub-license, we do not grant one for our embeds API.” And “Our platform policies require third parties to have the necessary rights from applicable rights holders. This includes ensuring they have a license to share this content, if a license is required by law.” “Instagram just threw users of its embedding API under the bus,” (June 4, 2020), available as of June 4, 2020 at <https://arstechnica.com/tech-policy/2020/06/instagram-just-threw-users-of-its-embedding-api-under-the-bus/>.

⁷²⁶ “Mashable Settles Copyright Fight Over Instagram Embeds,” *Law360* (Feb. 10, 2021), available as of Feb. 10, 2021 at www.law360.com/articles/1354269.

⁷²⁷ McGucken v. Newsweek LLC, 464 F. Supp. 3d 594, 599 (S.D.N.Y. 2020).

sublicense to Newsweek. None of Instagram’s various terms and policies expressly granted a sublicense to those who embed publicly posted content. Nor could the court find, on the pleadings, evidence of a possible implied sublicense. Given the limited review permitted at the motion to dismiss state, the court ruled that it could not find that Newsweek acted pursuant to a sublicense from Instagram.⁷²⁸

The court also rejected Newsweek’s motion to dismiss based on a fair use defense. The court not find as a matter of law that Newsweek’s use of the plaintiff’s photograph was transformative, noting that the lake itself was not the central subject of the article, so the photograph was incorporated into the article merely as an illustrative aid. In addition, Newsweek’s use of the photograph was commercial in nature. The court also noted that the Supreme Court has stated there is a preemption of market harm when a commercial use amounts to mere duplication of the entirety of an original. Accordingly, the court denied Newsweek’s motion to dismiss based on its alleged fair use of the photograph.⁷²⁹

In a subsequent opinion, the court rejected the server test. The plaintiff sought summary judgment on its claim for copyright infringement and willful infringement, such that the case would proceed to trial solely on the issue of damages. The defendant asked the court to find as a matter of law that the embedding of the Instagram post did not actually infringe any of the plaintiff’s exclusive rights, that it had a license to embed the plaintiff’s Instagram post, or alternatively, that its use of the Instagram post constituted fair use.⁷³⁰

The court rejected the defendant’s invocation of the server test. First, the court noted that the server test had not been widely adopted outside of the Ninth Circuit⁷³¹ and that other courts had persuasively argued that such a test may be contrary to the text and legislative history of the Copyright Act.⁷³² The court further observed that the Copyright Act defines “display” as “to show a copy of” a work and not “to make and then show a copy of the copyrighted work.”⁷³³ The Ninth Circuit’s approach, under which no display is possible unless the alleged infringer has also stored a copy of the work on the infringer’s computer, would seem to make the display right merely a subset of the reproduction right. The court found that the Copyright Act makes clear, however, that to “show a copy” is to display it. Moreover, under the server test, a copyright holder who promotes his work on Instagram would surrender control over how, when, and by whom the work is subsequently shown, reducing the display right, effectively, to the limited right of first publication that the Copyright Act of 1976 rejects.

⁷²⁸ Id. at 601-04.

⁷²⁹ Id. at 604-06, 609.

⁷³⁰ McGucken v. Newsweek LLC, 2022 U.S. Dist. LEXIS 50231 at *2 (S.D.N.Y. Mar. 21, 2022).

⁷³¹ Citing Goldman v. Breitbart News Network, LLC, 302 F. Supp. 3d 585, 591 (S.D.N.Y. 2018).

⁷³² Citing Nicklen v. Sinclair Broad. Grp., Inc., 2021 U.S. Dist. LEXIS 142768 (S.D.N.Y. 2021), discussed in the next subsection.

⁷³³ McGucken, 2022 U.S. Dist. LEXIS 50231 at *13 (citing Nicklen, 2021 U.S. Dist. LEXIS 142768 at *13).

Accordingly, the court concluded that the defendant did in fact display the plaintiff's photograph when it embedded the photograph in the Instagram article.⁷³⁴

The court also found that disputed issues of material fact prevented the granting of summary judgment on whether Instagram granted the defendant an express sublicense or implied sublicense and whether the defendant's use of the photograph constituted fair use. The court also denied the plaintiff's claim of willfulness since the plaintiff had not yet established liability for copyright infringement.⁷³⁵ In April of 2022 (less than a month after the court's ruling), Newsweek settled the dispute with the plaintiff.⁷³⁶

(6) Nicklen v. Sinclair Broad. Grp.

In this case, discussed in more detail in Section II.C.10 above, another district court in the S.D.N.Y. rejected the server test, finding it contrary to the text and legislative history of the copyright statute. The statute defines to display as "to show a copy of" a work, not "to make and then show a copy of the copyrighted work." The court found that the Ninth Circuit's approach, under which no display is possible unless the alleged infringer has also stored a copy of the work on the infringer's computer, therefore makes the display right merely a subset of the reproduction right. The court also believed that the Ninth Circuit's reasoning in the Perfect 10 case should be cabined by two facts specific to that case: (1) the defendant operated a search engine and (2) the copyrighted images were displayed only if a user clicked on a link in order to see the full image rather than merely the thumbnail that Google's search engine had displayed. The court also noted practical problems with the server test. Under that test, a photographer who promotes his work on Instagram or a filmmaker who posts her short film on YouTube surrenders control over how, when, and by whom their work is subsequently shown – reducing the display right, effectively, to the limited right of first publication that the Copyright Act of 1976 rejects.⁷³⁷

D. The Right of Public Distribution

Section 106 (3) of the copyright statute grants the copyright owner the exclusive right to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending. Thus, to implicate the right of public distribution, three conditions must obtain: (a) a "copy" must be distributed; (b) the distribution must be to the "public"; and (c) the distribution must be by sale, rental, lease, lending or "other transfer of ownership."

⁷³⁴ McGucken, 2022 U.S. Dist. LEXIS 50231 at *13-14.

⁷³⁵ Id. at *36.

⁷³⁶ Adam Lidgett, "Newsweek To Settle Instagram Embed Copyright Suite," *Law360* (April 14, 2022), available as of April 15, 2022 at www.law360.com/ip/articles/1483999/.

⁷³⁷ Nicklen v. Sinclair Broad. Grp., 2021 U.S. Dist. LEXIS 142768 at *12-15 (S.D.N.Y. July 30, 2021).

1. The Requirement of a “Copy”

Whether transmissions of a work on the Internet implicate the public distribution right turns in the first instance on whether there has been a distribution of a “copy” of the work. The broadcasting and cable industries have traditionally treated broadcasts and cable transmissions as *not* constituting distributions of copies of a work. With respect to Internet transmissions, however, if a complete copy of a work ends up on the recipient’s computer, it may be easy to conclude that a “copy” has been distributed. Indeed, to remove any doubt from this issue, the NII White Paper proposed to include “transmission” within the copyright owner’s right of distribution,⁷³⁸ where transmission is defined essentially as the creation of an electronic copy in a recipient system.⁷³⁹

It is less clear whether other types of transmissions constitute distributions of “copies.” For example, what about an artistic work that is transmitted and simultaneously performed live at the recipient’s end? Although the public performance right may be implicated, has there been a distribution of a “copy” that would implicate the right of distribution? Should it matter whether significant portions of the work are buffered in memory at the recipient’s computer? Many of these distinctions could be rendered moot by the potentially broader right of “communication to the public” contained in the WIPO treaties discussed below, were that right ever to be expressly adopted in implementing legislation in the United States (the DMCA does not contain such a right).

Even if a “copy” is deemed to have been distributed in the course of an Internet transmission of an infringing work, difficult questions will arise as to who should be treated as having made the distribution – the original poster of the unauthorized work, the OSP or BBS through which the work passes, the recipient, or some combination of the foregoing? Thus, the same issue of volition arises with respect to the distribution right as was discussed above in connection with the reproduction right.

(a) Cases Addressing Whether Mere “Making Available” Is a Distribution

Many decisions have addressed the question of whether the mere posting – i.e., the “making available” – of a work on a BBS or other Internet site, or in a “shared file” folder within peer-to-peer client software, from which it can be downloaded by members of the public constitutes a public distribution of the work, and have reached quite contrary results, as detailed in the next two subsections. In addition to those decisions, as detailed in the third subsection

⁷³⁸ The copyright statute currently defines “transmission” or “transmit” solely in reference to performances or displays of a work. The NII White Paper does not, however, argue for removal of the requirement that an offending distribution be one to the “public.” NII White Paper at 213-15.

⁷³⁹ NII White Paper at 213. Appendix 1 of the NII White Paper proposes the following definition: “To ‘transmit’ a reproduction is to distribute it by any device or process whereby a copy or phonorecord of the work is fixed beyond the place from which it was sent.” *Id.* App. 1, at 2.

below, several other decisions have declined to reach the issue and/or left the question open, often acknowledging the existence of conflicting authority.

(1) Cases Holding That Mere “Making Available” Is a Distribution

(i) Playboy Enterprises v. Frena

In Playboy Enterprises, Inc. v. Frena,⁷⁴⁰ the court, with very little analysis of the issue, held a BBS operator liable for infringement of the public distribution right for the making of photographs available through the BBS that were downloaded by subscribers, even though the defendant claimed he did not make copies of the photographs himself. But because the BBS was apparently one devoted to photographs, much of it of adult subject matter, and subscribers routinely uploaded and downloaded images therefrom, the court seems to have viewed the defendant as a direct participant in the distributions to the public that took place through the BBS.

(ii) Playboy Enterprises v. Chuckleberry Publishing

Similarly, in Playboy Enterprises, Inc. v. Chuckleberry Publishing Inc.,⁷⁴¹ the court ruled that uploading copyrighted pictorial images onto a computer in Italy which could be accessed by users in the United States constituted a public distribution in the United States. In contrast to the Netcom case, the court noted that the defendant did more than simply provide access to the Internet. Instead, the defendant provided services and supplied the content for those services, which gave users the option to either view or download the images. By actively soliciting United States customers to the services, the court concluded that the defendant had distributed its product within the United States.

(iii) Playboy Enterprises v. Webbworld

In Playboy Enterprises, Inc. v. Webbworld, Inc.,⁷⁴² the court held the defendants directly liable for infringing the distribution right by making copyrighted images available through a website for downloading by subscribers. The court found that, in contrast to the Netcom case, the defendants took “affirmative steps to cause the copies to be made.”⁷⁴³

⁷⁴⁰ 839 F. Supp. 1552 (M.D. Fla. 1993).

⁷⁴¹ 939 F. Supp. 1032, 1039 (S.D.N.Y. 1996).

⁷⁴² 45 U.S.P.Q.2d 1641 (N.D. Tex. 1997).

⁷⁴³ Id. at 1647.

(iv) Marobie-FL v. National Association of Fire Equipment

Distributors

The court in Marobie-FL, Inc. v. National Association of Fire Equipment Distributors⁷⁴⁴ ruled that the placement of three files containing copyrighted clip art on the Web page of the defendant constituted a direct violation of the plaintiff's distribution right because the files were available for downloading by Internet users and were transmitted to Internet users upon request.

In all of the preceding four cases in subsections (i) through (iv) above, it was apparent that actual downloads of complete copies of the copyrighted material had taken place, and this fact, coupled with affirmative steps taken by the defendants to promote the acts of downloading, seem to have led those courts to find a violation of the distribution right. The more difficult cases of line drawing have arisen in the peer-to-peer file sharing cases, many of which are discussed in the remainder of this subsection and the next subsection, in which the defendant often merely makes available copyrighted files for sharing (through a "shared file" folder used by the peer-to-peer client software), but does not take additional affirmative steps to promote the downloading of copies of those files. In addition, there often is not clear proof in those cases whether actual downloads have taken place from the defendant's particular shared file folder, and if so, to what extent – including whether complete copies have been downloaded from the defendant's shared file folder or only bits and pieces of files, as is the inherent nature of the peer-to-peer protocol mechanisms.

(v) A&M Records v. Napster

In its decision in Napster I, the Ninth Circuit held, without any discussion, that "Napster users who upload files names to the search index for others to copy violate plaintiff's distribution rights."⁷⁴⁵ Although the Ninth Circuit's opinion addressed whether Napster could be secondarily liable for the infringing acts of its users through the system, it did not address the question of whether Napster itself directly violated the plaintiff's distribution rights by maintaining its search index. That question was subsequently adjudicated by the district court in the Napster litigation, which answered the question in the negative, as discussed in the next subsection.

(vi) Interscope Records v. Duty

In Interscope Records v. Duty,⁷⁴⁶ the court held that the mere placement of copyrighted works in a share folder connected to the Kazaa peer-to-peer service constituted a public distribution of those works. The court noted that, although "distribute" is not defined in the copyright statute, the right of distribution is synonymous with the right of publication, which is defined to include the "*offering* to distribute copies or phonorecords to a group of persons for

⁷⁴⁴ 45 U.S.P.Q.2d 1236 (N.D. Ill. 1997).

⁷⁴⁵ A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1014 (9th Cir. 2001) (emphasis added).

⁷⁴⁶ 2006 U.S. Dist. LEXIS 20214 (D. Ariz. Apr. 14, 2006).

purposes of further distribution, public performance, or public display.”⁷⁴⁷ The court also cited the Ninth Circuit’s decision in Napster I, which held that “Napster users who upload files names to the search index for others to copy violate plaintiff’s distribution rights.”⁷⁴⁸

(vii) Warner Bros. Records v. Payne

In Warner Bros. Records, Inc. v. Payne,⁷⁴⁹ the court ruled, on a motion to dismiss the plaintiff’s complaint against a defendant who was making the plaintiff’s recordings available through the Kazaa network, that “[l]isting unauthorized copies of sound recordings using an online file-sharing system constitutes an offer to distribute those works, thereby violating a copyright owner’s exclusive right of distribution.”⁷⁵⁰ The court relied on the Supreme Court’s equating of the term “distribute” with “publication” in Harper & Row Publishers, Inc. v. Nation Enterprises,⁷⁵¹ noting that publication is defined to include the “offering to distribute copies.” The court also relied on the logic of Hotaling v. Church of Jesus Christ of Latter-Day Saints,⁷⁵² which held a library engages in the distribution of a copyrighted work when it adds the work to its collections, lists the work in its index or catalog and makes the work available for borrowing or browsing.⁷⁵³ Accordingly, the court denied the defendant’s motion to dismiss: “Making an unauthorized copy of a sound recording available to countless users of a peer-to-peer system for free certainly contemplates and encourages further distribution, both on the Internet and elsewhere. Therefore, the Court is not prepared at this stage of the proceedings to rule out the Plaintiffs’ ‘making available’ theory as a possible ground for imposing liability. A more detailed understanding of the Kazaa technology is necessary and Plaintiffs may yet bring forth evidence of actual uploading and downloading of files, rendering use of the ‘making available’ theory unnecessary.”⁷⁵⁴

(viii) Universal City Studios v. Bigwood

In Universal City Studios Productions v. Bigwood,⁷⁵⁵ the court granted summary judgment of infringement against the defendant, a user of Kazaa who had made two of the plaintiffs’ copyrighted motion pictures available in his shared folder. Citing Hotaling and Napster I and no contrary authority, and without any further analysis of its own, the court ruled that “by using

⁷⁴⁷ Id. at *7 (citing 17 U.S.C. § 101) (emphasis by the court).

⁷⁴⁸ Id. at *8 (quoting A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1014 (9th Cir. 2001)).

⁷⁴⁹ 2006 U.S. Dist. LEXIS 65765 (W.D. Tex. July 17, 2006).

⁷⁵⁰ Id. at *8.

⁷⁵¹ 471 U.S. 539 (1985).

⁷⁵² 118 F.3d 199 (4th Cir. 1997).

⁷⁵³ 2006 U.S. Dist. LEXIS at *9-10.

⁷⁵⁴ Id. at *11.

⁷⁵⁵ 441 F. Supp. 2d 185 (D. Me. 2006).

KaZaA to make copies of the Motion Pictures available to thousands of people over the internet, Defendant violated Plaintiffs' exclusive right to distribute the Motion Pictures."⁷⁵⁶

(ix) Motown Record Co. v. DePietro

In Motown Record Co. v. DePietro,⁷⁵⁷ the court, citing the Ninth Circuit's Napster I case, held that a "plaintiff claiming infringement of the exclusive-distribution right can establish infringement by proof of actual distribution or by proof of offers to distribute, that is, proof that the defendant 'made available' the copyrighted work [in this case, via a peer-to-peer system]."⁷⁵⁸

(x) United States v. Carani

In United States v. Carani,⁷⁵⁹ the court ruled that storing child pornography in a shared folder on the Kazaa peer-to-peer network where it could be downloaded by others qualified as an illegal "distribution" of child pornography, thus justifying an enhanced punishment.⁷⁶⁰

(xi) ICG-Internet Commerce Group v. Wolf

In ICG-Internet Commerce Group, Inc. v. Wolf,⁷⁶¹ the court denied a motion for summary judgment that the defendant had infringed the plaintiff's distribution right in an adult video by posting the video to the defendant's web site, because it was unclear from a screenshot of the defendant's web site showing a hyperlink to "[s]ex tape download sources [sic]" whether the hyperlink linked to a streaming or downloadable source file containing the plaintiff's video. The court did, however, find that the plaintiff's copy and public display rights had been violated by the posting of the video on the defendant's site from which it could be viewed publicly.⁷⁶²

(xii) Maverick Recording Co. v. Harper

In Maverick Recording Co. v. Harper,⁷⁶³ in considering a copyright infringement claim against the defendant for having copies of the plaintiffs' copyrighted sound recordings in a shared folder on a peer-to-peer network, the court held that a complete download of a given work over the network is not required for copyright infringement to occur. Citing the Warner Bros. v. Payne and Interscope decisions, the court stated, "The fact that the Recordings were

⁷⁵⁶ Id. at 190.

⁷⁵⁷ 2007 U.S. Dist. LEXIS 11626 (E.D. Pa. Feb. 16, 2007).

⁷⁵⁸ Id. at *12.

⁷⁵⁹ 492 F.3d 867 (7th Cir. 2007).

⁷⁶⁰ Id. at *21-23; accord United States v. Shaffer, 472 F.3d 1219, 1123-24 (10th Cir. 2007).

⁷⁶¹ 519 F. Supp. 2d 1014 (E.D. Pa. 2007).

⁷⁶² Id. at 1018-19.

⁷⁶³ Order, Maverick Recording Co. v. Harper, No. 5:07-CV-026-XR (W.D. Tex. Aug. 7, 2008).

available for download is sufficient to violate Plaintiffs' exclusive rights of reproduction and distribution. It is not necessary to prove that all of the Recordings were actually downloaded; Plaintiffs need only prove that the Recordings were available for download due to Defendant's actions."⁷⁶⁴

On appeal, the Fifth Circuit ruled that it need not address whether merely making available files for download violates the distribution right because the defendant did not appeal the district court's finding that she had infringed the plaintiffs' copyrights by downloading and therefore reproducing the audio files. Thus, the distribution issue was moot since the defendant's liability would remain even if the Fifth Circuit were to agree with the district court on the distribution issue.⁷⁶⁵ The Fifth Circuit also ruled that the defendant was not entitled to an innocent infringer defense as a matter of law because Section 402(d) makes that defense unavailable when a proper copyright notice appears on the published phonorecords to which a defendant had access. There was no dispute that each of the published phonorecords from which the shared audio files were taken had proper copyright notices on them, and lack of legal sophistication as to what the notices meant was irrelevant.⁷⁶⁶ (The court does not mention whether the audio files themselves that the defendant shared had copyright notices on them.) Accordingly, the court concluded that the plaintiffs must be awarded statutory damages of \$750 per infringed work.⁷⁶⁷

(xiii) **Columbia Pictures v. Fung**

In Columbia Pictures Industries, Inc. v. Fung,⁷⁶⁸ the district court ruled, in the context of a BitTorrent site, that "uploading a copyrighted content file to other users (regardless of where those users are located) violates the copyright holder's § 106(3) distribution right."⁷⁶⁹ Because of the nature of the BitTorrent protocol, users were not uploading the infringing content itself to the defendants' site, but rather were uploading dot-torrent files that contained only information about hosts from which the infringing content could be downloaded using the BitTorrent protocol. The dot-torrent files were indexed on the defendants' site for searching. Thus, the quoted language seems to implicitly hold that an actual distribution of infringing content is not required to infringe the distribution right, since the mere upload of the dot-torrent file through which the infringing content could be located was sufficient to infringe. In its opinion affirming on appeal, the Ninth Circuit stated, "Both uploading and downloading copyrighted material are infringing acts. The former violates the copyright holder's right to distribution, the latter the right to reproduction."⁷⁷⁰ The court immediately thereafter indicated awareness that the dot-

⁷⁶⁴ Id., slip op. at 10.

⁷⁶⁵ Maverick Recording Co. v. Harper, 598 F.3d 193, 197 (5th Cir. 2010).

⁷⁶⁶ Id. at 198-99.

⁷⁶⁷ Id. at 199.

⁷⁶⁸ 2009 U.S. Dist. LEXIS 122661 (C.D. Cal. Dec. 21, 2009), aff'd, 710 F.3d 1020 (9th Cir. 2013).

⁷⁶⁹ Id. at *29.

⁷⁷⁰ Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1034 (9th Cir. 2013).

torrent files that were uploaded to Fung’s web sites did not contain the infringing content itself, for the Ninth Circuit noted the plaintiff’s expert had averred that 90 to 96% of the content “associated with” the torrent files available on Fung’s web sites was for confirmed or highly likely copyright infringing material.⁷⁷¹

(xiv) SA Music v. Apple

In this case, the court concluded that Apple’s placement of infringing recordings or promotional clips on the iTunes Store could qualify as distribution under the Copyright Act. The court began by noting that the scope of a “making available” theory of copyright infringement has resulted in several decades of disagreement and debate among courts. The court began its analysis by noting that the statutory definition of the distribution right as referencing a distribution “by sale” could be read to mean that the only act of infringement possible is if the defendant makes a sale (and so too with transfer, rental, leasing, and lending). But the court noted the right might also reasonably be understood to be infringed by making the work available for sale (or transfer, rental, lease or lending) because that too interferes with exclusivity of distribution by sale and the other categories. Accordingly, the court treated the statute as at least ambiguous and turned to other interpretive tools.⁷⁷²

The court found the clearest indication that the distribution right includes “making available” recordings is that the modern copyright statute implements the World Intellectual Property Organization Copyright Treaty, and that Treaty explicitly covers a making available theory and grounds it in the distribution right. Specifically, the Treaty provides that “authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them.” The court noted that one explicit purpose of Congress’ adoption of the DMCA was to implement the Treaty. The court cited Supreme Court authority for the proposition that, when a statute implements a treaty, judicial interpretation begins with that international agreement. The court further noted that during the drafting of the Treaty there was robust discussion about the making available right – the United States argued that the distribution right covered a making available theory, so states should be able to enforce the right either through a stand-alone provision or through pre-existing rights. In drafting the DMCA, the Copyright Office studied the issue and told Congress that the existing rights were adequate to fulfill the Treaty obligations. And the House Report on the bill concluded the same thing.⁷⁷³

⁷⁷¹ Id.

⁷⁷² SA Music LLC v. Apple, Inc., 2022 U.S. Dist. LEXIS 50427 at *36-37 (N.D. Cal. Mar. 21, 2022). The court did not address the fact that the exclusive distribution right is defined in terms of the right to distribute “copies” or “phonorecords,” each of which is defined as “material objects.” 17 U.S.C. § 101.

⁷⁷³ Id. at *37-40.

The court also noted that the Ninth Circuit in the Napster case⁷⁷⁴ understood “distribution” in the Copyright Act to include making works available, and a more recent Ninth Circuit decision had reaffirmed and relied on that holding when the central question was about the scope of the distribution right.⁷⁷⁵ The court pointed to the fact that the Copyright Office, in a 2016 Report, reached the view that distribution can include uploading material to a database for consumers to peruse and choose whether or not to download or buy. And it is the view endorsed by the Nimmer copyright treatise and has been adopted by the Tenth Circuit and the Fourth Circuit.⁷⁷⁶ The court recognized that another district court judge within the Ninth Circuit’s jurisdiction reached a contrary conclusion in the case of SA Music, LLC v. Amazon.com, Inc.,⁷⁷⁷ distinguishing the Napster case on the ground that a service like Amazon’s music store required payment before download, whereas Napster’s users put up files that anyone could download without payment. But the instant court believed that nothing in the reasoning of Napster turned on the free nature of the product, holding instead, without qualification, that when a user uploaded a file for others to copy, it “distributed.” Accordingly, the court denied Apple’s motion for summary judgment on the plaintiff’s claim for liability on a “making available” theory.⁷⁷⁸

(2) Cases Holding That Mere “Making Available” Is Not a Distribution

(i) Religious Technology Center v. Netcom

In Religious Technology Center v. Netcom On-Line Communication Services,⁷⁷⁹ the court refused to hold either an OSP or a BBS operator liable for violation of the public distribution right based on the posting by an individual of infringing materials on the BBS. With respect to the BBS, the court stated: “Only the subscriber should be liable for causing the distribution of plaintiffs’ work, as the contributing actions of the BBS provider are automatic and

⁷⁷⁴ A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1014 (9th Cir. 2001) as amended (Apr. 3, 2001).

⁷⁷⁵ SA Music, 2022 U.S. Dist. LEXIS 50427 at *40 (citing Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1162 (9th Cir. 2007)).

⁷⁷⁶ SA Music, 2022 U.S. Dist. LEXIS 50427 at *40-41.

⁷⁷⁷ 2020 U.S. Dist. LEXIS 103373 at *7 (W.D. Wash. June 12, 2020).

⁷⁷⁸ SA Music, 2022 U.S. Dist. LEXIS 50427 at *41-42, *44. The court did, however, grant summary judgment for Apple on the plaintiff’s claim of willful infringement, finding that Apple reasonably relied on a representation from uploaders that they had adequate rights and that Apple had implemented a notice-and-takedown procedure designed to remove any composition when one party asserted rights and the uploader was not willing to challenge that assertion within five days. Id. at *14-36. The court noted that the plaintiffs never used the notice-and-takedown procedure, strongly indicating that Apple lacked actual knowledge of the alleged infringement. Id. at *16-17. The court also denied summary judgment for the plaintiffs on their direct infringement claims because there were genuine disputes of fact as to whether Apple’s behavior satisfied the “volitional conduct” requirement of copyright law. The court noted that the plaintiffs had introduced no evidence that Apple exercised sufficient control or discretion, or that it engaged in instigation, sufficient to entitle them to summary judgment – indeed, the plaintiffs’ motion did not address the volitional conduct requirement at all. Id. at *61-66.

⁷⁷⁹ 907 F. Supp. 1361, 1372 (N.D. Cal. 1995).

indiscriminate.”⁷⁸⁰ With respect to the OSP, the court noted: “It would be especially inappropriate to hold liable a service that acts more like a conduit, in other words, one that does not itself keep an archive of files for more than a short duration.”⁷⁸¹

(ii) In re Napster Copyright Litigation

In In re Napster, Inc. Copyright Litigation,⁷⁸² the district court rejected the plaintiffs’ argument that Napster’s indexing of MP3 files that its users posted on the Napster network made Napster a direct infringer of the plaintiffs’ exclusive distribution rights. The plaintiffs relied on Hotaling v. Church of Jesus Christ of Latter-Day Saints,⁷⁸³ which held a library engages in the distribution of a copyrighted work when it adds the work to its collections, lists the work in its index or catalog and makes the work available for borrowing or browsing. The Napster court distinguished the Hotaling case, arguing that the library had itself made actual, unauthorized copies of copyrighted materials made available to its borrowers. By contrast, Napster did not itself have a “collection” of recordings on its servers, but rather merely an index of recordings.⁷⁸⁴ “This might constitute evidence that the listed works were available to Napster users, but it is certainly not conclusive proof that the songs identified in the index were actually uploaded onto the network in a manner that would be equivalent to the way in which the genealogical materials at issue in Hotaling were copied and distributed to the church’s branch libraries.”⁷⁸⁵

The court further noted that the definition of “publication” in the copyright statute, which the Supreme Court observed in a 1985 case that the legislative history equated with the right of distribution,⁷⁸⁶ requires the distribution of copies or phonorecords of a work to the public or the offering to distribute copies of that work for purposes of further distribution, public performance, or public display. The court held that merely by indexing works available through its system, Napster was not offering to itself distribute copies of the works for further distribution by its users.⁷⁸⁷

The plaintiffs argued that the requirement of a transmission of a material object in order to find a violation of the distribution right was no longer viable in view of the recently enacted Artists’ Rights and Theft Prevention Act of 2005 (the ART Act).⁷⁸⁸ The plaintiffs cited Section 103(a)(1)(C) of the ART Act, codified at 17 U.S.C. § 506(a), which provides criminal sanctions for

⁷⁸⁰ Id. at 1372.

⁷⁸¹ Id.

⁷⁸² 377 F. Supp. 2d 796 (N.D. Cal. 2005).

⁷⁸³ 118 F.3d 199 (4th Cir. 1997).

⁷⁸⁴ In re Napster, Inc. Copyright Litigation, 377 F. Supp. 2d at 802-03.

⁷⁸⁵ Id. at 803.

⁷⁸⁶ Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 539 (1985).

⁷⁸⁷ In re Napster, Inc. Copyright Litigation, 377 F. Supp. 2d at 803-05.

⁷⁸⁸ Pub. L. No. 109-9, 119 Stat. 218 (2005).

any person who willfully infringes a copyright by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public. The plaintiffs interpreted this provision as imposing criminal liability on any person who willfully makes an unauthorized copy of a copyrighted work available on a publicly accessible computer network while that work is being prepared for commercial distribution, and argued that Congress must have understood civil liability for copyright infringement to be equally broad.⁷⁸⁹

The court rejected this argument, noting that the ART Act did not amend Section 106(3) of the copyright statute, and in any event Section 103(a)(1)(C) of the ART Act makes clear that willful copyright infringement and making the work available on a computer network are separate elements of the criminal offense. Hence, the mere making available of an unauthorized work on a computer network should not be viewed as sufficient to establish a copyright infringement.⁷⁹⁰ Accordingly, the court ruled that the defendants were entitled to summary judgment on the issue of direct liability on Napster's part by virtue of its index.⁷⁹¹ However, note that the Ninth Circuit's earlier decision in Napster I held that "Napster users [as opposed to Napster itself] who upload files names to the search index for others to copy violate plaintiff's distribution rights."⁷⁹²

(iii) Perfect 10 v. Google

In Perfect 10 v. Google,⁷⁹³ discussed in detail in Section II.C.4 above, the district court ruled that Google did not publicly distribute infringing copies of Perfect 10's copyrighted images that could be located through the Google Image Search function. "A distribution of a copyrighted work requires an 'actual dissemination' of copies. ... In the internet context, an actual dissemination means the transfer of a file from one computer to another. Although Google frames and inline links to third-party infringing websites, it is *those* websites, not Google, that transfer the full-size images to users' computers [upon clicking on a thumbnail version of the image displayed in the Google search results]. Because Google is not involved in the

⁷⁸⁹ In re Napster, Inc. Copyright Litigation, 377 F. Supp. 2d at 804.

⁷⁹⁰ Id. at 804-05.

⁷⁹¹ Id. at 805. The court held, however, that the plaintiffs had submitted sufficient evidence of direct infringement by Napster's users in the form of a showing of massive uploading and downloading of unauthorized copies of works, together with statistical evidence strongly suggesting that at least some of the plaintiffs' copyrighted works were among them. Id. at 806. "It may be true that the link between such statistical evidence of copyright infringement and the uploading or downloading of specific copyrighted works is at the moment a weak one. However, to avoid summary judgment, plaintiffs need only establish that triable issue of material fact preclude entry of judgment as a matter of law. ... Here in particular, the court is mindful of the fact that the parties have not even completed discovery relating to issues of copyright ownership and infringement." Id. at 806-07.

⁷⁹² A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1014 (9th Cir. 2001).

⁷⁹³ 416 F. Supp. 2d 828 (C.D. Cal. 2006), aff'd sub nom. Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1169 (9th Cir. 2007).

transfer, Google has not actually disseminated – and hence, [] has not distributed – the infringing content.”⁷⁹⁴

On appeal, the Ninth Circuit affirmed this ruling. Because Google’s search engine communicated only HTML instructions telling a user’s browser where to find full size images on web site, and Google did not itself distribute copies of the infringing photographs, Google did not have liability for infringement of the right of distribution with respect to full size images that could be located and displayed through the Image Search function.⁷⁹⁵ Perfect 10 argued that, under the Napster I and Hotaling cases discussed above, the mere making available of images violates the copyright owner’s distribution right. The Ninth Circuit held that this “deemed distribution” rule did not apply to Google, because, unlike the users of the Napster system or the library in Hotaling, Google did not own a collection of stored full size images that it made available to the public.⁷⁹⁶

(iv) **Latin American Music Co. v. Archdiocese of San Juan**

In Latin American Music Co. v. Archdiocese of San Juan,⁷⁹⁷ although not a case involving online activity, the First Circuit held that the defendant’s mere listing in its licensing catalog of songs that it did not own the copyright for did not constitute infringement. The court ruled that mere authorization of an infringing act is insufficient basis for copyright infringement, as infringement depends upon whether an actual infringing act, such as copying or performing, has taken place.⁷⁹⁸

(v) **London-Sire Records v. Doe**

In London-Sire Records, Inc. v. Doe 1,⁷⁹⁹ the court ruled that merely listing recordings as available for downloading on a peer-to-peer service did not infringe the distribution right. The court held that authorizing a distribution is sufficient to give rise to liability, but only if an infringing act occurs after the authorization.⁸⁰⁰ The court rejected the plaintiff’s argument to the contrary based on the Supreme Court’s equating of the term “distribute” with “publication” in Harper & Row Publishers, Inc. v. Nation Enterprises.⁸⁰¹ The court noted that the Supreme Court stated only that Section 106(3) recognized for the first time a distinct statutory right of first publication, and quoted the legislative history as establishing that Section 106(3) gives a

⁷⁹⁴ Id. at 844 (citing In re Napster, Inc. Copyright Litigation, 377 F. Supp. 2d 796, 802-04 (N.D. Cal. 2005)).

⁷⁹⁵ Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1162 (9th Cir. 2007).

⁷⁹⁶ Id. at 1162-63. Cf. National Car Rental Sys. v. Computer Assocs. Int’l, Inc., 991 F.2d 426, 434 (8th Cir. 1993) (stating that infringement of the distribution right requires the actual dissemination of copies or phonorecords).

⁷⁹⁷ 499 F.3d 32 (1st Cir. 2007).

⁷⁹⁸ Id. at 46-47.

⁷⁹⁹ 542 F. Supp. 2d 153 (D. Mass. 2008).

⁸⁰⁰ Id. at 166.

⁸⁰¹ 471 U.S. 539 (1985).

copyright holder the right to control the first public distribution of an authorized copy of his work.⁸⁰² The court went on to state, however, “That is a far cry from squarely holding that publication and distribution are congruent.”⁸⁰³

The court noted that the statutory language itself suggests the terms are not synonymous. Noting that “publication” incorporates “distribution” as part of its definition (“publication” is “the distribution of copies or phonorecords of a work to the public”), the court reasoned:

By the plain meaning of the statute, all “distributions ... to the public” are publications. But not all publications are distributions to the public – the statute explicitly creates an additional category of publications that are not themselves distributions. For example, suppose an author has a copy of her (as yet unpublished) novel. If she sells that copy to a member of the public, it constitutes both distribution and publication. If she merely offers to sell it to the same member of the public, that is neither a distribution nor a publication. And if the author offers to sell the manuscript to a publishing house “for purposes of further distribution,” but does not actually do so, that is a publication but not a distribution.⁸⁰⁴

Accordingly, the court concluded that the defendants could not be liable for violating the plaintiffs’ distribution right unless a “distribution” actually occurred.⁸⁰⁵ But that conclusion, did not, however, mean that the plaintiffs’ pleadings and evidence were insufficient: “The Court can draw from the Complaint and the current record a reasonable inference in the plaintiffs’ favor – that where the defendant has completed all the necessary steps for a public distribution, a reasonable fact-finder may infer that the distribution actually took place.”⁸⁰⁶

The court also made the following additional rulings:

-- That the Section 106(3) distribution right is not limited to physical, tangible objects, but also confers on copyright owners the right to control purely electronic distributions of their work. The court reasoned that electronic files are “material objects” in which a sound recording can be fixed, and electronic distributions entail the movement of such electronic files, thereby implicating the distribution right.⁸⁰⁷

-- That actual downloads of the plaintiffs’ works made by the plaintiffs’ investigator were “sufficient to allow a statistically reasonable inference that at least one copyrighted work was

⁸⁰² London-Sire, 542 F. Supp. 2d at 168.

⁸⁰³ Id.

⁸⁰⁴ Id. at 169.

⁸⁰⁵ Id.

⁸⁰⁶ Id.

⁸⁰⁷ Id. at 169-71 & 172-74.

downloaded at least once [by persons other than the investigator]. That is sufficient to make out a prima facie case for present purposes.”⁸⁰⁸

(vi) **Elektra Entertainment Group v. Barker**

In Elektra Entertainment Group, Inc. v. Barker,⁸⁰⁹ contrary to the London-Sire Records decision (which incidentally was decided on the same day), the court ruled that, based on the legislative history of the copyright statute and the Supreme Court’s Harper & Row decision, the words “distribution” and “publication” should be construed as synonymous, and therefore the right of distribution should be equated to the right of publication.⁸¹⁰ Accordingly, the court ruled that the same acts that would constitute a publication as defined in Section 101 of the copyright statute – namely, the “offer[] to distribute copies or phonorecords to a group of persons for purposes of further distribution, public performance, or public display” – would also violate the distribution right, and that proof of an actual transfer need not be shown.⁸¹¹

However, the court rejected the plaintiff’s argument that a violation of the distribution right could be established by a mere showing of the “making available” of copyrighted works by the defendant, as the plaintiffs had pled in their complaint. The court rejected the plaintiffs’ argument that Congress’ adoption of the WIPO Copyright Treaty, which contains an express right of “making available” a copyrighted work to the public, should control the interpretation of Section 106(3)’s distribution right. The court noted that, because the WIPO treaties were not self-executing, they created no private right of action on their own. The court was also unwilling to infer the intent of an earlier Congress when enacting amendments to the definition of the distribution right from the acts of a later Congress in ratifying the WIPO Copyright Treaty.⁸¹² Accordingly, the court was unwilling to equate Congress’ words, that the distribution right may be infringed by “[t]he offer[] to distribute copies or phonorecords to a group of person for purposes of further distribution, public performance, or public display,” to what the court described as “the contourless ‘make available’ right proposed by Plaintiff.”⁸¹³

The court also rejected the argument in an amicus brief submitted by the MPAA that the plaintiffs’ “make available” claim was supported by the introductory clause of Section 106, which gives the owner of a copyright the exclusive right “to authorize” the enumerated rights. The court cited and followed authority noting that Congress had added the “authorize” language to

⁸⁰⁸ Id. at 176. “As noted above, merely exposing music files to the internet is not copyright infringement. The defendants may still argue that they did not know that logging onto the peer-to-peer network would allow others to access these particular files, or contest the nature of the files, or present affirmative evidence rebutting the statistical inference that downloads occurred.” Id.

⁸⁰⁹ 551 F. Supp. 2d 234 (S.D.N.Y. 2008).

⁸¹⁰ Id. at 239-41.

⁸¹¹ Id. at 242 (quoting 17 U.S.C. § 101’s definition of “publication”).

⁸¹² Id. at 242 n.7.

⁸¹³ Id. at 243.

Section 106 in order to avoid any confusion that the statute was meant to reach contributory infringers, not to create a separate basis for direct infringement.⁸¹⁴

The court did, however, give the plaintiffs the opportunity to amend their complaint to be faithful to the language of the copyright statute by alleging that the defendant had made an offer to distribute, and that the offer to distribute was for the purpose of further distribution, public performance, or public display.⁸¹⁵ In addition, the court denied the defendant's motion to dismiss the complaint entirely because the plaintiffs had adequately alleged that, in addition to making their works available, the defendant had actually distributed the plaintiffs' copyrighted works in direct violation of the distribution right.⁸¹⁶ In August of 2008 the case settled.⁸¹⁷

(vii) **Atlantic Recording Corp. v. Howell**

In Atlantic Recording Corp. v. Howell,⁸¹⁸ seven major recording companies brought suit against the defendants, who had allegedly made over 4,000 files available for download in a shared folder on Kazaa. The private investigation company MediaSentry took screen shots showing the files that were available for download. The plaintiffs owned registered copyrights in 54 of the sound recordings in the folder. MediaSentry downloaded 12 of the copyrighted recordings from the defendants' computer, and the plaintiffs traced the computer to the defendants and filed an action for copyright infringement. The plaintiffs filed a motion for summary judgment of infringement.⁸¹⁹

The court denied the motion. Citing numerous decisions and two copyright treatises, the court noted the general rule that infringement of the distribution right requires an actual dissemination of either copies or phonorecords. The court rejected the plaintiffs' reliance on the Hotaling case and the Ninth Circuit's Napster I decision. With respect to Hotaling, the court noted that in that case the plaintiff had already proved that the library made unlawful copies and placed them in its branch libraries, so there had been actual distributions of copies in addition to listing of the unlawful copies in the library's catalog. With respect to the Napster I decision, the court noted that the Ninth Circuit in the later Perfect 10 v. Amazon case had grouped the holdings of Hotaling and Napster I together based upon the factual similarity that in both cases the owner of a collection of works made them available to the public. Only in such a situation could the holding of Hotaling potentially apply to relieve the plaintiff of the burden to prove actual dissemination of an unlawful copy of a work. The defendant in the Perfect 10 case did not

⁸¹⁴ Id. at 245-46.

⁸¹⁵ Id. at 244-45.

⁸¹⁶ Id. at 245.

⁸¹⁷ "RIAA Settles Pending 'Making Available' Claim," *BNA's Electronic Commerce & Law Report* (Aug. 27, 2008) at 1160.

⁸¹⁸ 554 F. Supp. 2d 976 (D. Ariz. 2008).

⁸¹⁹ Id. at 978.

own a collection of copyrighted works or communicate them to the public, so the Ninth Circuit found Hotaling inapplicable.⁸²⁰ The Howell court went on to note the following:

However, the court did hold that “the district court’s conclusion [that distribution requires an ‘actual dissemination’] is consistent with the language of the Copyright Act.” That holding contradicts Hotaling and casts doubt on the single unsupported line from Napster upon which the recording companies rely.⁸²¹

After surveying the many decisions addressing the issue, the court concluded that it agreed “with the great weight of authority that § 106(3) is not violated unless the defendant has actually distributed an unauthorized copy of the work to a member of the public. ... Merely making an unauthorized copy of a copyrighted work available to the public does not violate a copyright holder’s exclusive right of distribution.”⁸²² In reaching its conclusion, the court rejected the plaintiffs’ argument that “distribution” and “publication” are synonymous terms in the statute for all purposes. Rather, the court noted it was not clear that “publication” and “distribution” are synonymous outside the context of first publication, which was the subject of discussion in the Supreme Court’s Harper & Row decision. Citing London-Sire, the court noted that while all distributions to the public are publications, not all publications are distributions.⁸²³ The court concluded: “A plain reading of the statute indicates that a publication can be either a distribution or an offer to distribute for the purposes of further distribution, but that a distribution must involve a ‘sale or other transfer of ownership’ or a ‘rental, lease, or lending’ of a copy of the work.”⁸²⁴

Finally, the court noted that the plaintiffs’ motion for summary judgment must also fail because they had not proved that a Kazaa user who places a copyrighted work into the shared folder distributes a copy of that work when a third party downloads it. The court noted that in the Kazaa system the owner of the shared folder does not necessarily ever make or distribute an unauthorized copy of the work. And if the owner of the shared folder simply provides a member of the public with access to the work and the means to make an unauthorized copy, the owner would not be liable as a primary infringer of the distribution right, but rather would be potentially liable only as a secondary infringer of the reproduction right.⁸²⁵ The court therefore concluded that the plaintiffs’ motion for summary judgment must fail because “they have not explained the architecture of the KaZaA file-sharing system in enough detail to determine conclusively whether the owner of the shared folder distributes an unauthorized copy (direct

⁸²⁰ Id. at 981-82.

⁸²¹ Id. at 982 (quoting Perfect 10 v. Amazon.com, Inc., 487 F.3d 701, 718 (9th Cir. 2007) (superseded by 508 F.3d 1146 (9th Cir. 2007))).

⁸²² 554 F. Supp. 2d at 983.

⁸²³ Id. at 984.

⁸²⁴ Id. at 985.

⁸²⁵ Id. at 986.

violation of the distribution right), or simply provides a third-party with access and resources to make a copy on their own (contributory violation of the reproduction right).”⁸²⁶

(viii) Capitol Records v. Thomas

In Capitol Records Inc. v. Thomas,⁸²⁷ the court sua sponte raised the issue of whether it had erred in instructing the jury that making sound recordings available for distribution on a peer-to-peer network, regardless of whether actual distribution was shown, qualified as distribution under the copyright act. The court concluded that it had erred and ordered a new trial for the defendant.⁸²⁸ The parties agreed that the only evidence of actual dissemination of copyrighted works was that plaintiffs’ infringement policing agent, MediaSentry, had downloaded songs. The defendant argued that dissemination to an investigator acting as an agent for the copyright owner cannot constitute infringement. The court rejected this argument, noting that Eighth Circuit precedent clearly approved of the use of investigators by copyright owners, and distribution to an investigator can constitute infringement.⁸²⁹

The court then turned to the issue of whether merely making available recordings for download constitutes unauthorized distribution. The court first noted that the plain language of Section 106(3) does not state that making a work available for sale, transfer, rental, lease or lending constitutes distribution, and two leading copyright treatises (Nimmer and Patry) agree that making a work available is insufficient to establish distribution. Congress’ choice not to include offers to do the acts enumerated in Section 106(3) further indicated its intent that an actual distribution or dissemination is required by Section 106(3).⁸³⁰

The court rejected the holding of other courts that the definition of “distribution” should be taken to be the same as that of “publication,” noting that the legislative history does not expressly state that distribution should be given the same broad meaning as publication, and in any case, even if the legislative history indicated that some members of Congress equated publication with distribution under Section 106(3), that fact could not override the plain meaning of the statute. The court concluded that the statutory definition of publication is broader than the term “distribution” as used in Section 106(3). Specifically, under the definition in Section 101, a publication can occur by means of the distribution of copies of a work to the public, but it can also occur by offering to distribute copies to a group of persons for purposes of further distribution, public performance, or public display. Thus, while a publication effected by

⁸²⁶ Id.

⁸²⁷ 579 F. Supp. 2d 1210 (D. Minn. 2008).

⁸²⁸ Id. at 1212 & 1227. The instruction to the jury read: “The act of making copyrighted sound recordings available for electronic distribution on a peer-to-peer network, without license from the copyright owners, violates the copyright owners’ exclusive right of distribution, regardless of whether actual distribution has been shown.” Id. at 1212.

⁸²⁹ Id. at 1214-15.

⁸³⁰ Id. at 1217-18.

distributing copies of the work is a distribution, a publication effected by merely offering to distribute copies to the public is merely an offer of distribution, an actual distribution.⁸³¹

The court rejected the plaintiffs' argument that Section 106 affords an exclusive right to authorize distribution (based on Section 106's language that "the owner of copyright under this title has the exclusive rights to do and to authorize any of the following ...") and that making sound recordings available on a peer-to-peer network would violate such an authorization right. The court concluded that the authorization clause merely provides a statutory foundation for secondary liability, not a means of expanding the scope of direct infringement liability. The court reasoned that if simply making a copyrighted work available to the public constituted a distribution, even if no member of the public ever accessed that work, copyright owners would be able to make an end run around the standards for assessing contributory copyright infringement.⁸³²

Finally, the court rejected the arguments of the plaintiffs and various amici that the WIPO treaties require the U.S. to provide a making-available right and that right should therefore be read into Section 106(3). The court noted that the WIPO treaties are not self-executing and lack any binding legal authority separate from their implementation through the copyright act. The contents of the WIPO treaties would be relevant only insofar as Section 106(3) was ambiguous, and there was no reasonable interpretation of Section 106(3) that would align with the United States' treaty obligations. Concern for compliance with the WIPO treaties could not override the clear congressional intent in the language of Section 106(3).⁸³³

The defendant in this case, Jammie Thomas-Rasset, ultimately became the first peer-to-peer file sharer to defend infringement litigation all the way to a jury verdict. In July 2007, a jury concluded that she should pay \$220,000 in statutory damages, but she was granted a motion for a new trial based on the erroneous jury instruction discussed above. In the second trial, the jury returned a verdict for \$1.92 million. The court later reduced the award to \$54,000 but granted the plaintiffs' request for a new trial on damages. After a third trial, the jury again returned a special verdict that included a statutory damages award of \$1.5 million (\$62,500 for each shared song, multiplied by 24 songs).⁸³⁴

(ix) Fox Broadcasting v. Dish Network

In *Fox Broadcasting Co. v. Dish Network LLC*,⁸³⁵ the court rejected Fox's argument that the mere "making available" of Fox's programming to subscribers was sufficient to constitute a distribution. The district court observed that, while neither the Ninth Circuit nor any other

⁸³¹ *Id.* at 1219-20.

⁸³² *Id.* at 1220-21.

⁸³³ *Id.* at 1225-26.

⁸³⁴ "On Third Shot, Jury Returns \$1.5 Million Statutory Damages Verdict Against P2P User," *BNA's Electronic Commerce & Law Report* (Nov. 10, 2010) at 1692.

⁸³⁵ 106 F. Supp. 3d 1139 (C.D. Cal. 2015).

circuit court had addressed the “make available” theory of distribution under the copyright statute, it had been considered by a number of courts, and the great majority of courts that had considered the question had stopped short of fully endorsing the “make available” right. The district court found those cases persuasive and concluded that Dish’s act of merely “making available” copyrighted programming to its subscribers through its Prime Time Anytime (PTAT) service did not amount to distribution without actual dissemination.⁸³⁶ (For a detailed discussion of this case, see Section II.A.4(u) above.)

(x) BMG v. Cox Communications

For the reasons discussed in Section III.C.2(w) below, the district court in this case ruled that the distribution right does not include the mere “making available” of a copyrighted work for sale or other transfer of ownership, rental, lease or lending.

(xi) Alticor v. UMG Recordings

In Alticor Inc. v. UMG Recordings, Inc.⁸³⁷ several defendant recording companies sought in a counterclaim to hold the plaintiffs in this declaratory judgment action liable for direct, vicarious and contributory infringement based on alleged unauthorized digital audio transmissions of the defendants’ sound recordings contained in videos uploaded to the Internet by several independent business owners who were supervised and regulated by the plaintiffs as part of an international multi-level marketing company. The plaintiffs argued that the court should dismiss any of the defendants’ claims to the extent based on allegations that the defendants’ recordings were made available to the public by uploading the videos to the Internet. The court noted that, although it agreed the copyright statute does not confer a “making available” right under Section 106, the act of making a copyrighted work available for the use of a direct infringer was relevant to the defendants’ claims of indirect infringement as it could provide circumstantial evidence of actual disseminations by the direct infringers. Accordingly, the court denied the plaintiffs’ motion to dismiss with respect to the defendants’ “making available” argument.⁸³⁸

⁸³⁶ Id. at 1169-70.

⁸³⁷ 2015 U.S. Dist. LEXIS 166317 (M.D. Fla. Dec. 11, 2015).

⁸³⁸ Id. at *4, *16 & *20. The court also rejected the plaintiffs’ arguments that the defendants could not bring a claim for infringement of the digital audio transmission right because the infringed sound recordings were contained within videos, which the plaintiffs argued were “audiovisual works” to which Section 106(6) does not apply because Section 114(j)(5) supposedly excludes “audiovisual work” from the definition of “digital audio transmission.” The court rejected the plaintiffs’ arguments on two grounds. First, the court was not persuaded that the definition of “digital audio transmission” in Section 114(j)(5) is applicable to an infringement analysis under Section 106(6) because Section 114(j) states that the definitions in that section are for use in that section only. Second, the sound recordings constituted preexisting material upon which the videos, as derivative works, were based, and Section 106(3) provides that copyright protection in preexisting material is not affected by use of such material in a derivative work. Id. at *16-19.

(xii) APL Microscopic v. United States

In this case, the plaintiff APL Microscopic alleged that NSAS infringed its copyrights by posting APL's copyrighted photo on a web page within NASA's website in 2004. The government moved to dismiss because APL alleged only one act of infringement of the rights of reproduction, public display and public distribution that occurred in 2004, outside the three-year statute of limitations. This defense required the court to adjudicate whether NASA infringed by merely making the work available on its server for download and display in 2004, or only upon actual distributions and viewings by the public, which were ongoing activities within the statute of limitations.⁸³⁹

With respect to the distribution right, the government contended the right of distribution is implicated when copies of a work are made available to the public, such as placed on the server and available for download, and does not depend on whether members of the public have accessed the distribution by downloading the work. The government analogized to Section 506(a)(1), which sets forth criminal penalties for willful copyright infringement "if the infringement was committed by the distribution of a work being prepared for commercial distribution, *by making it available* on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution."⁸⁴⁰ The court rejected this argument, finding persuasive the reasoning to the contrary of the district court's decision in BMG v. Cox (discussed in Section II.D.1(a)(2)(x) above). In addition, the court noted there is good reason to construe the language of Sections 106(3) and 506(a)(1)(C) separately, because criminal offenses and civil offenses are treated differently. The court held that infringement of the right of public distribution under Section 106(3) requires actual dissemination of either copies or phonorecords. The court therefore denied the government's motion to dismiss APL's claim of infringement of its right of distribution.⁸⁴¹

With respect to the public display right, the government argued that the right is implicated when the work is placed on display for viewing by the public, such as placed on the server and accessible via the web site, and does not depend on whether members of the public have in fact viewed the work, such as by accessing the page. The court disagreed, noting that the Copyright Act unambiguously defines display of a work as "to show a copy of it, either directly or by means of a film, slide, television image, or any other device or process"⁸⁴² The definition's use of "any other device or process" clearly brings showing a copy of a work through a computer within the statutory definition of "display." Thus, each unauthorized showing of a work through a computer infringes on the owner's right of public display. Accordingly, each time a user viewed on his or her computer NASA's web page after the work was published on the NASA site in 2004, there was a separate infringement of APL's right of public display, with each

⁸³⁹ APL Microscopic, LLC v. United States, 144 Fed. Cl. 489, 491496 (Ct. Cl. 2019).

⁸⁴⁰ Id. at 496 (quoting 17 U.S.C. § 506(a)(1)(C) (emphasis added)).

⁸⁴¹ Id. at 497-98.

⁸⁴² Id. at 498 (quoting 17 U.S.C. § 101).

infringement starting a new limitations period. The court therefore denied the government's motion to dismiss APL's claims of infringement of its right of public display.⁸⁴³

(xiii) SA Music v. Amazon.com

The plaintiffs, owners of copyrights in musical compositions, alleged that Amazon violated their distribution right by making available on the Amazon store unauthorized copies of recordings based on their songs. Amazon moved for summary judgment on this claim. The court granted the motion, concluding that under the definition of "distribution" in the copyright statute, a distribution must involve a sale or other transfer of ownership or a rental, lease, or lending of a copy of the copyrighted work – in other words, an actual dissemination of either copies or phonorecords or the transfer of a file containing the copy from one computer to another.⁸⁴⁴ The court rejected the plaintiffs' analogy to the Hotaling case,⁸⁴⁵ in which the Fourth Circuit found that copyrighted material listed in the index or catalog of a public library was deemed distributed. While such indexing in a catalog may be analogous to making a work available to the public through a file-sharing network, the court found it is not analogous to requiring a customer to pay for the work before a download can occur.⁸⁴⁶

The court also rejected the plaintiffs' contention that distribution is equivalent to publication, noting that "publication" is defined more broadly in the statute than "distribution" to include both distribution of physical copies to the public by sale or other transfer or rental, lease or lending, and offering to distribute copies to a group of persons for purposes of further distribution, public performance or public display. Thus, although all distributions to the public are publications, not all publications are distributions, and there was no allegation that Amazon made an offer to distribute the unauthorized copies of the copyrighted compositions for the purpose of further distribution, public performance, or public display. The court therefore granted Amazon's motion to dismiss as to the plaintiffs' claim for "making available for sale unauthorized copies of [unauthorized] recordings in violation of exclusive distribution rights under 17 U.S.C. § 106(3)."⁸⁴⁷

(xiv) Brittney Gobble Photography v. Sinclair Broadcasting

In this case, the plaintiff sought to rely on the Hotaling decision to argue the defendants should be held liable under the distribution right because the defendants had included the plaintiff's photographs in articles stored on their content management systems. The court, citing the BMG v. Cox Communications case (discussed in Section II.D.1(a)(2)(x) above), among others, rejected this broad reading of Hotaling, agreeing with those cases that Hotaling's "making

⁸⁴³ Id. at 498-99.

⁸⁴⁴ SA Music, LLC v. Amazon.com, Inc., 2020 U.S. Dist. LEXIS 103373 at *5-8 (W.D. Wa. June 12, 2020), motion for reconsideration denied, U.S. Dist. LEXIS 118616 (W.D. Wa. July 7, 2020).

⁸⁴⁵ Hotaling v. Church of Jesus Christ of Latter-Day Saints, 118 F.3d 199 (4th Cir. 1997).

⁸⁴⁶ SA Music, 2020 U.S. Dist. LEXIS 103373 at *11-12.

⁸⁴⁷ Id. at *17-19.

available” decision did not announce a rule of general applicability, but instead articulated a principle that applies only in cases where it is impossible for a copyright owner to produce proof of actual distribution. Here, proof of actual distribution was not impossible for the plaintiff to demonstrate. Under Section 610(3) of the copyright statute, infringement of the distribution right requires an actual dissemination of either copies or phonorecords. Because the plaintiff had not attempted to offer evidence of actual distribution, the court granted summary judgment to the defendants on the plaintiff’s claim for violation of the distribution right.⁸⁴⁸

(xv) Grecco v. Age Fotostock Am.

The plaintiff discovered mis-attributed versions of four of his photographs on a website owned by the defendant’s Spanish parent company, where they were displayed and offered to the public for licensing. Upon receiving notice of the infringing photos through the parent’s U.S. subsidiary, the parent notified the plaintiff that the photos had been taken down and that neither the parent nor its U.S. subsidiary had licensed or made any sales of the photos. The plaintiff then sued the U.S. subsidiary, arguing that it was directly liable for infringing the plaintiff’s copyrights on the ground that the offer to license photos for the express purpose of further reproduction and publication of them constituted direct infringement, even though no license was ever sold by the defendant and the images were never downloaded in the United States.⁸⁴⁹

The court granted summary judgment to the defendant with respect to the direct infringement claim. The court observed that under the statutory language of Section 106(3), distribution requires dissemination of a “copy,” which is defined as a “material object ... in which a work is fixed.” The court noted that, relying on this language, several other courts had held that an unconsummated offer to sell a copyrighted work does not constitute infringement under the Copyright Act.⁸⁵⁰ The court found these decisions persuasive, and authority to the contrary not persuasive.⁸⁵¹

⁸⁴⁸ Brittney Gobble Photography, LLC v. Sinclair Broad. Grp., Inc., 2021 U.S. Dist. LEXIS 222009 at *59-61 (D. Md. Nov. 17, 2021).

⁸⁴⁹ Grecco v. Age Fotostock Am., Inc., 2021 U.S. Dist. LEXIS 192021 at *3, *7 & *9 (S.D.N.Y. Oct. 5, 2021).

⁸⁵⁰ Id. at *10-11, citing Obolensky v. G.P. Putnam’s Sons, 628 F. Supp. 1552, 1555-56 (S.D.N.Y. 1986) (“The courts have held that there is no violation of the right to vend copyrighted works ... where the defendant offers to sell copyrighted materials but does not consummate a sale”) and the Capitol Records v. Thomas and Atlantic Recording Corp. v. Howell cases, discussed in Sections II.D.1(a)(2)(viii) and (vii) above, respectively.

⁸⁵¹ Id. at *11-13, rejecting the reasoning of the court in Elektra Ent. Grp., Inc. v. Barker, 551 F. Supp. 2d 234, 243 (S.D.N.Y. 2008), which stated, in the context of rejecting the plaintiff’s bid to recognize an even broader “make available” right under the Copyright Act, that even an unconsummated offer can violate the distribution right of Section 106(3). The Grecco court rejected the Elektra court’s reliance on the Supreme Court’s decision in Harper & Row Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 552 (1985), which the Elektra court (erroneously in the Grecco court’s view) characterized as having found “distribution” and “publication” (which does not require actual distribution of physical copies) to be synonymous. Given that the statute defines “publication” to include both distribution and offers to distribute, the Grecco court concluded that, while all

(3) Cases Refusing To Decide the Issue

- In Arista Records LLC v. Greubel, 453 F. Supp. 2d 961 (N.D. Tex. 2006), the court, although not deciding on a motion to dismiss whether the electronic transmission over a computer network (here, transmission of copyrighted recordings through a file sharing network) or the mere listing of such copyrighted recordings in a directory as available for download, is sufficient to violate a copyright owner’s distribution right, the court cited numerous decisions so holding or suggesting that either of such acts is sufficient for infringement of the distribution right, and concluded that such decisions were sufficient to deny the defendant’s motion to dismiss the complaint on the pleadings.⁸⁵² The court stated, “[M]aking copyrighted works available to others *may* constitute infringement by distribution *in certain circumstances*.”⁸⁵³
- Maverick Recording Co. v. Goldshteyn, 2006 U.S. Dist. LEXIS 52422 at *3 (E.D.N.Y. July 31, 2006) (“[T]he ‘making available’ argument need not be decided here.”).
- Fonovisa, Inc. v. Alvarez, 2006 U.S. Dist. LEXIS 95559 at *8 (N.D. Tex. July 24, 2006) (“This Court is not making a determination as to whether ‘making works available’ violates the right of distribution.”).
- Warner Bros. Records, Inc. v. Payne, 2006 U.S. Dist. LEXIS 65765 at *4 (W.D. Tex. July 17, 2006) (declining to “rule out the Plaintiffs’ ‘making available’ theory as a possible ground for imposing liability”).
- Atlantic Recording Corp. v. Brennan, 2008 U.S. Dist. LEXIS 23801 at *3 (D. Conn. Feb. 13, 2008) (denying plaintiffs’ entry of default against defendant, in part, by finding that defendant may have a meritorious defense against plaintiffs’ “problematic” make available argument).
- Electra Entertainment Group, Inc. v. Doe, 2008 U.S. Dist. LEXIS 98145 at *8-9 (E.D.N.C. Dec. 4, 2008) (court need not decide whether “making available” a sound recording over the Internet constitutes a distribution because the plaintiffs’ complaint sufficiently alleged an actual dissemination of copies of the recordings had occurred).
- Warner Bros. Records, Inc. v. Doe, 2008 U.S. Dist. LEXIS 98143 at *8-9 (E.D.N.C. Dec. 4, 2008) (same).
- In Arista Records LLC v. Does 1-16, 2009 U.S. Dist. LEXIS 12159 (N.D.N.Y. Feb. 18, 2009), several record labels brought a copyright infringement claim against 16 unidentified defendants

distributions to the public are publications, not all publications are distributions. The court also rejected the plaintiff’s reliance on a Sept. 25, 2002 letter from the Register of Copyrights supporting the conclusion in Elektra, noting that letters from the Copyright Office to Congress on matters of statutory interpretation are entitled to respect only insofar as they are persuasive. Id. at *11 n.4.

⁸⁵² Id. at 967-71.

⁸⁵³ Id. at 969 (emphasis added).

for illegally downloading and distributing the plaintiffs' copyrighted music through a peer-to-peer network and issued a subpoena seeking information from the State University of New York at Albany sufficient to identify each defendant. The defendants sought to quash the subpoena, in part on the basis that the plaintiffs' complaint was defective in that, in essence, according to the defendants, it alleged that the defendants were infringers because they were making available copyrighted song files, but without any evidence of actual distribution of those files to the public. The court refused to decide whether the mere "making available" of song files would be sufficient to violate the distribution right because the complaint did not use that language, but rather alleged that each defendant downloaded and/or distributed to the public copies of sound recordings.⁸⁵⁴ "We are persuaded by the majority of cases and the school of thought that Plaintiffs have adequately pled that Defendants distributed Plaintiffs' copyrighted work, by merely stating, within the four corners of the Complaint, the distribution allegation alone. The tasks of pleading and proving that each Defendant actually distributed the copyright work do not necessarily collide at this juncture of the case, and dismissal of the Complaint would not be appropriate at this stage."⁸⁵⁵

– VHT, Inc. v. Zillow Group, Inc., 2017 U.S. Dist. LEXIS 95010 (W.D. Wash. June 20, 2017): See discussion of this case in Section III.C.1(i) below.

(b) Other Cases Adjudicating the Scope of the Distribution Right

(1) Hearst Stations v. Aereo

In Hearst Stations Inc. v. Aereo, Inc.,⁸⁵⁶ Aereo used antenna and DVR technology to transmit over-the-air television broadcasts over the Internet to its subscribers. The technology allowed users to watch programming live (with a few second delay) or to record it for viewing at a later time. In either case, when a user elected to watch a program, a small antenna (out of a large array of antennas) was assigned exclusively to that user for that time period to intercept the signal as the program was broadcast over-the-air and transmit it to the user's designated space on Aereo's hard drive. Aereo's system then converted the signal from its original format to a different digital format that allowed the user to access the program over the Internet. A user could access his or her individual copy of a program by streaming it over the Internet from Aereo's hard drive to his or her personal computer, smart phone, or other Internet-enabled device. The system did not permit users to download permanent physical copies of programs to their personal hard drives. The plaintiff contended, among other claims, that Aereo infringed its distribution right. The court rejected this claim, noting that although the Copyright Act does not define what it means to "distribute," a number of courts had interpreted it to entail an actual dissemination of either copies or phonorecords. Here, because Aereo's technology allowed

⁸⁵⁴ Id. at *15-16.

⁸⁵⁵ Id. at *16-17.

⁸⁵⁶ 2013 U.S. Dist. LEXIS (D. Mass. Oct. 8, 2013).

users only to stream but not download programming, Aereo was more aptly described as “performing” rather than “distributing” copyrighted works.⁸⁵⁷

(2) Fox Broadcasting v. Dish Network

The facts of Fox Broadcasting Co. v. Dish Network, L.C.C.⁸⁵⁸ are discussed in Section II.A.4(u) above. Among many other issues, the district court considered whether Dish was liable for violation of Fox’s distribution right and found that it was not. Citing the Perfect 10 v. Amazon case,⁸⁵⁹ the court noted that infringement of the distribution right requires actual dissemination of a copy by sale or other transfer of ownership, or by rental, lease, or lending. Here, a PTAT-enabled Hopper recorded primetime programming locally and, at most that local copy was disseminated within a single household. PTAT and AutoHop therefore did not involve any actual distribution of unauthorized copies, so the court concluded that Fox had not established a likelihood of success on the merits of its distribution claim.⁸⁶⁰ The distribution issue was not addressed in the Ninth Circuit’s affirming opinion on appeal.

In a subsequent opinion after discovery, the district court again ruled that PTAT did not “distribute” Fox’s programming because, as the court had previously held in its ruling on the first motion for a preliminary injunction, distribution under the copyright statute requires actual dissemination of a copy that changes hands. PTAT was a system for automatically recording programming as it was being received by a subscriber’s set-top box, inside the subscriber’s home. Those recordings were therefore not distributed, delivered, or transmitted to any other location or person using PTAT alone.⁸⁶¹

2. The Requirement of a “Public” Distribution

Unlike the case of the public performance and public display rights, the copyright statute does not define what constitutes a “public” distribution. However, one might expect courts to afford a similarly broad interpretation of “public” with respect to the right of public distribution. Some distributions will clearly be “public,” such as the posting of material on a Usenet newsgroup, and some will clearly not, such as sending e-mail to a single individual. Many other Internet distributions will fall in between. However, one might expect courts to treat distribution to members of the public by Internet access at different times and places as nevertheless “public,” by analogy to the public performance and public display rights.

⁸⁵⁷ Id. at *3-4, *17-18.

⁸⁵⁸ 905 F. Supp. 2d 1088 (C.D. Cal. 2012), aff’d (as amended), 747 F.3d 1060 (9th Cir. 2014).

⁸⁵⁹ Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1162 (9th Cir. 2007).

⁸⁶⁰ Fox Broadcasting, 905 F. Supp. 2d at 1106.

⁸⁶¹ Fox Broadcasting Co. v. Dish Network LLC, 160 F. Supp. 3d 1139, 1169-70 (C.D. Cal. 2015).

As previously discussed with respect to the public display right, the court in Playboy Enterprises, Inc. v. Hardenburgh,⁸⁶² held the defendant operators of a BBS directly liable for infringement of the public distribution right by virtue of making available photographs to subscribers of the BBS for a fee, many of which were copyrighted photographs of the plaintiff Playboy Enterprises. The court's basis for finding liability was derived principally from the fact that the defendants had a policy of encouraging subscribers to contribute files, including adult photographs, to an "upload file" on the BBS and the defendants' practice of using a screening procedure in which its employees screened all files in the upload file to remove pornographic material and moved them into the generally available files for subscribers. These facts led the court to conclude that the defendants were active participants in the process of copyright infringement.

With respect to the requirement that the distributions be "to the public" in order to infringe the distribution right, the court ruled that "Defendants disseminated unlawful copies of [the plaintiff's] photographs to the public by adopting a policy in which [the defendants'] employees moved those copies to the generally available files instead of discarding them."⁸⁶³ The court also concluded that the defendants were liable for contributory infringement by virtue of their encouraging of subscribers to upload information to the BBS with at least constructive knowledge that infringing activity was likely to be occurring on their BBS.⁸⁶⁴

3. The Requirement of a Rental or Transfer of Ownership

The public distribution right requires that there have been either a rental or a transfer of ownership of a copy. If material is distributed free, as much of it is on the Internet, there is no sale, rental, or lease, and it is therefore unclear whether a sale or a "transfer of ownership" has taken place. With respect to distributions in which the recipient receives a complete copy of the work on the recipient's computer, perhaps a "transfer of ownership" should be deemed to have taken place, since the recipient has control over the received copy.

It is unclear precisely what a "rental" means on the Internet. For example, is a download of an on-demand movie a "rental"? In a sense, the user pays a "rental" fee to watch the movie only once. However, the downloaded bits of information comprising the movie are never "returned" to the owner, as in the case of the usual rental of a copy of a work. These unanswered questions lend uncertainty to the scope of the distribution right on the Internet.

4. The Right of Distribution Under the WIPO Treaties

Article 6 of the WIPO Copyright Treaty provides that authors of literary and artistic works shall enjoy "the exclusive right of authorizing the making available to the public of the original and copies of their works through sale or other transfer of ownership." This right seems

⁸⁶² 982 F. Supp. 503 (N.D. Ohio 1997).

⁸⁶³ Id. at 513.

⁸⁶⁴ Id. at 514.

potentially broader than the public distribution right under current U.S. law, because it includes the mere “making available” of copies of works to the public, whereas U.S. law currently reaches only the actual distribution of copies.

It is unclear whether this “making available” right reaches the mere posting of copies on the Internet. The Agreed Statement for Article 6 provides: “As used in these Articles, the expressions ‘copies’ and ‘original and copies,’ being subject to the right of distribution and the right of rental under the said Articles, refer exclusively to fixed copies that can be put into circulation as tangible objects.” One interpretation of the Agreed Statement is that a copy posted on the Internet, being electronic in format, is not capable of being “put into circulation as tangible objects.”

On the other hand, one might argue that at least complete copies downloaded to permanent storage at recipient computers should be treated as the equivalent of circulation of copies “as tangible objects.” If, for example, copies of a book were sold on floppy disks rather than on paper, such floppy disks might well be treated as the placement of copies into circulation as tangible objects. Yet a network download can result in a copy on a floppy disk (or a hard disk) at the recipient’s computer. One could therefore argue that the transmission of electronic copies to “physical” storage media at the receiving end should be treated as within the distribution right of the WIPO treaty.

In any event, this “making available” right might more easily reach BBS operators and OSPs through which works are “made available” on the Internet. It is unclear whether a requirement of volition will be read into Article 6 for liability, as some U.S. courts have required for liability under the current rights of public distribution, display and performance. Moreover, because the WIPO Copyright Treaty does not define the “public,” the same ambiguities will arise as under current U.S. law concerning what type of availability will be sufficient to be “public,” particularly with respect to the “making available” of works to limited audiences.

Articles 8 and 12 of the WIPO Performances and Phonograms Treaty contain rights of distribution very similar to that of Article 6 of the WIPO Copyright Treaty,⁸⁶⁵ so the same ambiguities noted above will arise.

⁸⁶⁵ Article 8(1) provides, “Performers shall enjoy the exclusive right of authorizing the making available to the public of the original and copies of their performances fixed in phonograms through sale or other transfer of ownership.” Article 12(1) provides, “Producers of phonograms shall enjoy the exclusive right of authorizing the making available to the public of the original and copies of their phonograms through sale or other transfer of ownership.”

Like the Agreed Statement for the WIPO Copyright Treaty quoted in the text, the Agreed Statement for Articles 8 and 12 of the WIPO Performances and Phonograms Treaty provides: “As used in these Articles, the expressions ‘copies’ and ‘original and copies,’ being subject to the right of distribution and the right of rental under the said Articles, refer exclusively to fixed copies that can be put into circulation as tangible objects.”

5. The Right of Distribution Under WIPO Implementing Legislation

(a) United States Legislation

The DMCA does not contain any provisions that would modify the right of distribution as it exists under current United States law. Thus, the DMCA implicitly deems the current right of public distribution to be equivalent to the Article 6 right.

(b) The European Copyright Directive

Article 4(1) of the European Copyright Directive requires member states to “provide for authors, in respect of the original of their works or of copies thereof, the exclusive right to authorize or prohibit any form of distribution to the public by sale or otherwise.” Use of the phrase “any form” of distribution suggests that a broad right is intended, although, as in the United States, the right applies only with respect to the distribution of “copies.”⁸⁶⁶ Consistent with the Agreed Statement of the WIPO Copyright Treaty, the comments to Article 4(1) of the European Copyright Directive recite that “the expressions ‘copies’ and ‘originals and copies,’ being subject to the distribution right, refer exclusively to fixed copies that can be put into circulation as tangible objects.”⁸⁶⁷

Thus, although use of the phrase “any form” of distribution might suggest that all online transmissions of copyrighted works would fall within the distribution right of the European Copyright Directive, the comments limit the distribution right “to fixed copies that can be put into circulation as tangible objects.” It seems that the drafters of the European Copyright Directive intended the right of communication to the public, rather than the right of distribution, to cover online transmissions of copyrighted works, for Recital (23) states that the right of communication to the public “should be understood in a broad sense covering all communication to the public not present at the place where the communication originates. This right should cover any such transmission or retransmission of a work to the public by wire or wireless means, including broadcasting. This right should not cover any other acts.”

E. The Right of Importation

Section 602(a) of the copyright statute provides that “importation into the United States ... of copies or phonorecords of a work that have been acquired outside the United States is an infringement of the exclusive right to distribute copies” One purpose of Section 602(a) was to allow a copyright owner to prevent distribution into the United States of copies of works that, if made in the United States, would have been infringing, but were made abroad outside the reach of United States copyright law.

⁸⁶⁶ Art. 4(2) deals with exhaustion of the distribution right under the first sale doctrine, and will be discussed in Section III.F below.

⁸⁶⁷ Commentary to Art. 4, ¶ 1.

Section 602(a) was obviously drafted with a model of physical copies in mind. “Importation” is not defined in the copyright statute, but the requirement that copies of a work be “acquired outside the United States” might suggest that “importation” means the movement of physical copies into the United States.⁸⁶⁸ It is unclear how this right will be applied to Internet transmissions into the United States, with respect to which no physical copies in a traditional sense are moved across national borders. Because the NII White Paper takes the position that the stream of data sent during a transmission does not constitute a “copy” of a copyrighted work, the NII White Paper concludes that the Section 602(a) importation right does not apply to network transmissions into the United States,⁸⁶⁹ and recommends that Section 602 be amended to include importation by transmission of copies, as well as by carriage or shipping of them.⁸⁷⁰

However, because physical copies often end up on a computer in the United States as a result of network transmissions into the United States, it is possible that the importation right will be construed analogously to the distribution right with respect to transmissions, especially since the importation right is defined in Section 602(a) in terms of the distribution right. Thus, if a transmission is deemed to be within the distribution right, then it is possible that the importation right will be construed to apply when transmissions of copies are made into the United States from abroad.

In any event, the new right of communication to the public afforded under the WIPO treaties, discussed in the next section, could help plug any hole that may exist in the traditional importation right, at least with respect to transmissions into the United States that qualify as “communications to the public,” if the such right is adopted in implementing legislation (as noted in the next section, however, the DMCA does not contain an explicit right of communication to the public).

F. The New Right of Transmission and Access Under the WIPO Treaties

The WIPO treaties each afford a broad new right of transmission and access to a copyrighted work. The right is denominated a “right of communication to the public” in the WIPO Copyright Treaty, and is denominated a “right of making available to the public” in the WIPO Performances and Phonograms Treaty. Despite the difference in denomination, the rights appear to be very similar.

1. The Right of Communication to the Public in the WIPO Copyright Treaty

Article 8 of the WIPO Copyright Treaty provides a new right of “communication to the public” as follows:

⁸⁶⁸ Lemley, *supra* note 6, at 564.

⁸⁶⁹ NII White Paper at 68.

⁸⁷⁰ *Id.* at 135.

Without prejudice to the provisions of Articles 11(1)(ii), 11*bis*(1)(i) and (ii), 11*ter*(1)(ii), 14(1)(ii) and 14*bis*(1) of the Berne Convention, authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them.

This new extended right of communication to the public is clearly meant to cover online dissemination of works, and in that sense is broader than the existing rights of communication to the public in the Berne Convention, which are confined to performances, broadcasts, and recitations of works. Specifically, Article 11(1)(ii) of the Berne Convention provides that authors of dramatic, dramatico-musical and musical works shall enjoy the exclusive right of authorizing “any communication to the public of the performance of their works.” Article 11*bis*(1)(ii) provides that authors of literary and artistic works shall enjoy the exclusive right of authorizing “any communication to the public by wire or by rebroadcasting of the broadcast of the work, when this communication is made by an organization other than the original one.” Finally, Article 11*ter*(1)(ii) provides that authors of literary works shall enjoy the exclusive right of authorizing “any communication to the public of the recitation of their works.”

The new right of communication to the public in the WIPO Copyright Treaty appears to be broader than the existing rights of reproduction, display, performance, distribution, and importation under current United States law in the following ways:

- No Requirement of a Copy. The right does not require the making or distribution of “copies” of a work. It therefore removes the potential limitations on the rights of reproduction and distribution under United States law stemming from the requirement of a “copy.”
- Right of Transmission. It affords the exclusive right to control any “communication to the public” of a work “by wire or wireless means.” Although “communication” is not defined in the WIPO Copyright Treaty, the reference to a communication “by wire or wireless means” seems clearly applicable to electronic transmissions of works (a right of transmission). This conclusion is bolstered by the fact that Article 2(g) of the WIPO Performances and Phonograms Treaty does contain a definition of “communication to the public,” which is defined in terms of “transmission to the public by any medium, other than broadcasting.”⁸⁷¹ This transmission right will potentially site the infringement at the place of transmission, in addition to the point of receipt of a transmitted work (under the reproduction right).

⁸⁷¹ Article 2(f) of the WIPO Performances and Phonograms Treaty defines “broadcasting” to mean “the transmission by wireless means for public reception of sounds or of images and sounds or of the representations thereof” This definition seems to contemplate isochronous transmission.

- Right of Authorization. It also affords the exclusive right of “authorizing” any communication to the public. No actual communications to the public are apparently necessary to infringe the right.
- Right of Access. The right of authorizing communications to the public explicitly includes “making available to the public” a work “in such a way that members of the public may access” the work “from a place and a time individually chosen by them” (a right of access).⁸⁷² This access right would seem to allow the copyright holder to remove an infringing posting of a work prior to any downloading of that work. This right may also expand potential liability beyond just posters or recipients of infringing material on the Internet to include OSPs and BBS operators, who could be said to make a work available to the public in such a way that members of the public may access it.

The Agreed Statement for Article 8, however, appears aimed at limiting the breadth of the net of potential liability that Article 8 might establish. The Agreed Statement provides: “It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention. It is further understood that nothing in Article 8 precludes a Contracting Party from applying Article 11*bis*(2).” It is unclear who the “mere” provider of “physical facilities” was meant to reference – only the provider of telecommunications lines (such as phone companies) through which a work is transmitted, or other service providers such as OSPs or BBS operators, who may provide “services” in addition to “facilities.”

Another unclear point with respect to the scope of the right of communication to the public is who the “public” is. Neither the WIPO Copyright Treaty nor the European Copyright Directive provide any explanation of “to the public,” although the Commission in its 1997 commentary to one of the earlier drafts of the Directive stated that “public” included “individual members of the public,” but went on to state that “the provision does not cover mere private communications.”⁸⁷³

The right of transmission and access under Article 8 of the WIPO Copyright Treaty is similar to (and potentially broader than) the amendment to U.S. copyright law proposed in the NII White Paper “to expressly recognize that copies or phonorecords of works can be distributed to the public by transmission, and that such transmissions fall within the exclusive distribution right of the copyright owner.”⁸⁷⁴ The NII White Paper’s proposal would expand the distribution right, as opposed to creating a wholly new right, as the WIPO Copyright Treaty does. The

⁸⁷² Although “public” is not defined in the WIPO Copyright Treaty, the reference in Article 10 to access by members of the public “from a place and at a time individually chosen by them” is very similar to the definition of display or performance of a work “publicly” in Section 101 of the U.S. copyright statute, which applies “whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times.”

⁸⁷³ Harrington & Berking, *supra* note 308, at 4.

⁸⁷⁴ NII White Paper at 130.

amendment proposed by the NII White Paper proved to be very controversial, and implementing legislation introduced in Congress in 1996 ultimately did not win passage.

The European Court of Justice ruled on Mar. 7, 2013 that the right of communication to the public in the EU Copyright Directive covers any transmission or retransmission of a work to the public not present at the place where the communication originates, whether it be by wire or wireless means, including broadcasting. Thus, television broadcasters may prohibit the retransmission of their programs on the Internet by another company. The decision arose out of a case brought by U.K.-based commercial broadcaster ITV against TVCatchup Ltd., an Internet television service that offered many programs via live streaming. TVCatchup argued that it was not in violation of EU copyright law because its subscribers, all based in the U.K., had paid the annual TV license fee, the funds of which were used to finance public broadcasters such as the BBC and ITV. ITV sued in a U.K. court, which referred the case to the European Court of Justice to get an interpretation of what constitutes a “communication to the public.” The ECJ also ruled that authorizing the inclusion of protected works in a communication to the public does not exhaust the right to authorize or prohibit other communications to those works to the public. Accordingly, when a given work is put to multiple use, each transmission or retransmission of that work using a specific technical means must, as a rule, be individually authorized by the copyright owner. The ECJ concluded that because the production of a program made available through retransmission over the Internet uses a technology different from that of the original communication, the retransmission must be considered to be a “communication” within the meaning of the EU Copyright Directive.⁸⁷⁵

2. The Right of Making Available to the Public in the WIPO Performances and Phonograms Treaty

Articles 10 and 14 of the WIPO Performances and Phonograms Treaty grant analogous rights for performers and producers of phonograms to the right of “communication to the public” contained in Article 8 of the WIPO Copyright Treaty. The WIPO Performances and Phonograms Treaty, however, casts these rights as ones of “making available to the public.” Specifically, Article 10 of the WIPO Performances and Phonograms Treaty provides:

Performers shall enjoy the exclusive right of authorizing the making available to the public of their performances fixed in phonograms, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them.

⁸⁷⁵ Joe Kirwin, “Broadcaster Can Block Retransmission of Programs on Internet, EU High Court Says,” *BNA’s Patent, Trademark & Copyright Journal* (Mar. 12, 2013).

Thus, Article 10 provides an exclusive right with respect to analog and digital on-demand transmission of fixed performances.⁸⁷⁶

Similarly, Article 14 provides:

Producers of phonograms shall enjoy the exclusive right of authorizing the making available to the public of their phonograms, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them.

No Agreed Statements pertaining to Articles 10 and 14 were issued.

Article 2(b) of the WIPO Performances and Phonograms Treaty defines a “phonogram” to mean “the fixation of the sounds of a performance or of other sounds, or of a representation of sounds other than in the form of a fixation incorporated in a cinematographic or other audiovisual work.” Article 2(c) defines “fixation” broadly as “the embodiment of sounds, or of the representations thereof, from which they can be perceived, reproduced or communicated through a device.” Under this definition, storage of sounds on a computer would constitute a “fixation,” and the fixed copy of such sounds would therefore constitute a “phonogram.” Accordingly, the making available to the public of sounds stored on a computer would seem to fall within the access rights of Articles 10 and 14.

Because there were no Agreed Statements generated in conjunction with Sections 10 and 14 of the WIPO Performances and Phonograms Treaty, there is no Agreed Statement similar to that accompanying Article 8 in the WIPO Copyright Treaty for limiting liability for the mere provision of physical facilities for enabling or making transmissions. Accordingly, one will have to await the implementing legislation in the various countries to know how broadly the rights set up in Articles 10 and 14 will be codified into copyright laws throughout the world.

3. The Right of Transmission and Access Under WIPO Implementing Legislation

(a) United States Legislation

The DMCA does not contain any express implementation of a right of “communication to the public” or of “making available to the public.” In view of this, the uncertainties discussed previously concerning whether the mere transmission or access of a copyrighted work through

⁸⁷⁶ Rebecca F. Martin, “The WIPO Performances and Phonograms Treaty: Will the U.S. Whistle a New Tune?”, J. Copyright Soc’y U.S.A., Spring 1997, at 157, 178. Art. 8 provides a correlative distribution right with respect to more traditional forms of distribution: “Performers shall enjoy the exclusive right of authorizing the making available to the public of the original and copies of their performances fixed in phonograms through sale or other transfer of ownership.” The WIPO Performances and Phonograms Treaty also grants to authors in Art. 6 the exclusive right of authorizing “the broadcasting and communication to the public of their unfixed performances except where the performance is already a broadcast performance” as well as “the fixation of their unfixed performances.”

an online medium falls within existing United States rights of reproduction, distribution, public display, or public performance remain under the DMCA.

With respect to the Article 10 right of making available to the public of fixed performances, the Digital Performance Rights in Sound Recordings Act grants these rights for digital transmissions, although not for analog transmissions.⁸⁷⁷ However, because the WIPO Performances and Phonograms Treaty grants these rights with respect to both digital and analog transmissions, as well as with respect to spoken or other sounds in addition to musical works, it would seem that the United States might have to amend its copyright laws to comply with the requirements of Article 10.⁸⁷⁸

Although the DMCA does not contain any express rights of transmission or access, some early case law suggested that courts might interpret existing copyright rights to afford the equivalent of a right of transmission and access. For example, in Marobie-FL, Inc. v. National Association of Fire Equipment Distributors,⁸⁷⁹ discussed previously, the court concluded that the mere making available of the files for downloading was sufficient for liability, because “once the files were uploaded [onto the Web server], they were available for downloading by Internet users and ... the [OSP] server transmitted the files to some Internet users when requested.”⁸⁸⁰ From this statement, it appears that the court construed the distribution and public display rights to cover both the making available of the clip art to the public on the Web page (a right of access), as well as subsequent downloads by users (a right of transmission).

Many decisions since Marobie-FL have addressed the question whether the mere “making available” of a copyrighted work online constitutes an infringement of the distribution right under U.S. law and have reached contradictory results. See Section II.D.1(a) above.

(b) The European Copyright Directive

The European Copyright Directive explicitly adopts both the right of communication to the public of copyrighted works and the right of making available to the public of fixed performances, by wire or wireless means, in language that parallels that of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. Specifically, Article 3(1) of the European Copyright Directive provides the following with respect to copyrighted works:

Member States shall provide authors with the exclusive right to authorize or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them.

⁸⁷⁷ 17 U.S.C. § 106 (6).

⁸⁷⁸ Martin, supra note 876, at 178-79.

⁸⁷⁹ 45 U.S.P.Q.2d 1236 (N.D. Ill. 1997).

⁸⁸⁰ Id. at *12.

The comments to Article 3 define “communication to the public” to cover “any means or process other than the distribution of physical copies. This includes communication by wire or by wireless means,”⁸⁸¹ which clearly encompasses a right of transmission. Indeed, the comments explicitly note: “One of the main objectives of the provision is to make it clear that interactive ‘on-demand’ acts of transmissions are covered by this right.”⁸⁸² This theme is picked up in Recital (25) of the European Copyright Directive, which states, “It should be made clear that all rightholders recognized by this Directive should have an exclusive right to make available to the public copyright works or any other subject-matter by way of interactive on-demand transmissions. Such interactive on-demand transmissions are characterized by the fact that members of the public may access them from a place and at a time individually chosen by them.” Recital (27), however, echoes similar statements in the WIPO Copyright Treaty when it states that the “mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Directive.” The Recitals do not clear up the ambiguity previously noted in the WIPO Treaty as to who the “mere” provider of “physical facilities” was meant to reference – only the provider of telecommunications lines (such as phone companies) through which a work is transmitted, or other service providers such as OSPs or BBS operators.

The comments to the European Copyright Directive also make clear that Article 3(1) affords a right to control online access to a work, apart from actual transmissions of the work:

As was stressed during the WIPO Diplomatic Conference, the critical act is the “making available of the work to the public,” thus the offering a work on a publicly accessible site, which precedes the stage of its actual “on-demand transmission.” It is not relevant whether it actually has been retrieved by any person or not. The “public” consists of individual “members of the public.”⁸⁸³

Similarly, Article 3(2) of the European Copyright Directive affords a right of making available to the public of fixed performances by wire or wireless means:

Member States shall provide for the exclusive right to authorize or prohibit the making available to the public, by wire or wireless means, in such a way that members of the public may access them from a place and at a time individually chosen by them:

- (a) for performers, of fixations of their performances;
- (b) for phonogram producers, of their phonograms;

⁸⁸¹ Commentary to Art. 3, ¶ 1.

⁸⁸² Id. ¶ 2.

⁸⁸³ Id.

(c) for the producers of the first fixation of films, of the original and copies of their films;

(d) for broadcasting organizations, of fixations of their broadcasts, whether these broadcasts are transmitted by wire or over the air, including by cable or satellite.

The right of Article 3(2) of the European Copyright Directive is actually broader than the right required under Article 10 of the WIPO Performances and Phonograms Treaty. The Article 10 right of making available to the public applies only to performances fixed in “phonograms,” which Article 2 defines to mean the fixation of the “sounds of a performance or of other sounds other than in the form of a fixation incorporated in a cinematographic or other audiovisual work.” The Article 3(2) right of the European Copyright Directive goes further, covering fixed performances of audiovisual material as well. The comments to Article 3(2) of the European Copyright Directive justify this extension of the right on the ground that audiovisual productions or multimedia products are as likely to be available online as are sound recordings.⁸⁸⁴

In sum, the European Copyright Directive explicitly grants a right of transmission and access to copyrighted works and fixed performances, whereas the DMCA does not. It remains to be seen how broadly these rights mandated under the European Copyright Directive will be adopted in implementing legislation in EC member countries. However, this disparity between the express rights afforded under United States law and the European Copyright Directive raises considerable potential uncertainty. First, at a minimum, use of different language to denominate the various rights among countries may breed confusion. Second, differences of scope of the rights of transmission and access are likely to arise between the United States and the EC by virtue of the fact that these rights are spelled out as separate rights in the EC, whereas, if they exist at all, they are subsumed under a collection of various other rights in the United States. Adding further to the potential confusion is the possibility that some EC member countries may adopt these rights expressly, as mandated by the European Copyright Directive, whereas other countries may, like the United States, deem them to be subsumed in other rights already afforded under that country’s laws.

Because online transmissions through the Internet are inherently global, these disparities raise the possibility that rights of varying scope will apply to an online transmission as it travels through computers in various countries on the way to its ultimate destination. Similarly, legal rights of varying scope may apply depending upon in which country a work is actually first accessed. Given the ubiquitous nature of caching on the Internet, the site of the access may be arbitrary from a technical point of view, but significant from a legal point of view. Such a situation would not afford the international uniformity that the WIPO treaties seek to establish.

⁸⁸⁴ *Id.* ¶ 3.

G. New Rights and Provisions Under The Digital Millennium Copyright Act, the European Copyright Directive & Legislation That Did Not Pass

This Section discusses a number of new rights and provisions related to various areas of copyright law that are contained in the DMCA and the European Copyright Directive. In addition, this Section discusses a number of interesting rights and provisions concerning copyright in the online context that were contained in proposed legislation that did not pass Congress. These provisions are indicators of areas where future legislation and/or debate may arise.

1. Circumvention of Technological Measures and Rights Management Information Under the DMCA

Both the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty require signatories to establish certain obligations with respect to circumvention of technological measures to protect copyrighted works and the preservation and use of certain “rights management information.”

With respect to the circumvention of technological measures, Article 11 of the WIPO Copyright Treaty and Article 18 of the WIPO Performances and Phonograms Treaty require treaty signatories to “provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures” that are used by authors, performers and producers of phonograms to restrict acts with respect to their copyrighted works that are not authorized by the rights holders or permitted by law.⁸⁸⁵

With respect to the preservation and use of rights management information, Article 12 of the WIPO Copyright Treaty and Article 19 of the WIPO Performances and Phonograms Treaty require treaty signatories to provide adequate and effective legal remedies against any person performing any of the following acts knowing (or, with respect to civil remedies, having reasonable grounds to know) “that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention”: (i) removing or altering any electronic rights management information without authority or (ii) distributing, importing for distribution, broadcasting or communicating to the public, without authority, copies of works knowing that electronic rights management information has been removed or altered without authority. The treaties define “rights management information” as “information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such

⁸⁸⁵ Shortly after the WIPO treaties were adopted, Assistant Secretary of Commerce and Commissioner of Patents and Trademarks Bruce Lehman, who headed the U.S. delegation at the WIPO Conference, noted that this provision is somewhat broader than the statutory language proposed on the subject in Congress before adoption of the treaties. He noted that implementation of this treaty provision would therefore require new legislation. “WIPO Delegates Agree on Two Treaties,” *BNA’s Electronic Information Policy & Law Report* (Jan. 3, 1997) at 23.

information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.”

This subsection 1 discusses the implementation of these rights in the DMCA. The following subsection 2 discusses the implementation of these rights under the European Copyright Directive.

The four bills that were introduced in Congress to implement the WIPO treaties adopted one of two approaches to the circumvention of technological measures and rights management information. The first approach, contained in H.R. 2281 and S. 2037 and ultimately adopted in the DMCA, outlawed both conduct and devices directed toward or used for circumventing technological copyright protection mechanisms. The second approach, contained in S. 1146 and H.R. 3048 but not passed by Congress, outlawed only conduct involving the removal or deactivation of technological protection measures. Although Bruce Lehman conceded that the WIPO treaties do not mandate adoption of a device-based approach, he and other supporters of this approach argued that a conduct-only approach would be difficult to enforce and that meaningful legislation should control the devices used for circumvention.⁸⁸⁶

The DMCA adds several new provisions to the Copyright Act, which are contained in a new Chapter 12.

(a) Circumvention of Technological Protection Measures

(1) Prohibition on Conduct

Section 1201(a)(1) of the DMCA outlaws conduct to circumvent protection mechanisms that control access to a copyrighted work: “No person shall circumvent a technological measure that effectively controls access to a work protected under this title.” Note that this provision does not expressly require either knowledge or intent, and is therefore potentially very broad in its reach – the language states that the mere act of circumvention is a violation, and does not expressly require that an infringement follow the circumvention act (although some courts have grafted such a requirement as discussed below). Section 1201(a)(3) defines “circumvent a technological measure” as “to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner.” That section further provides that a technological protection measure “effectively controls access to a work” if “the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.”

Section 1201(a)(1) provides that the prohibition on circumventing a technological measure to gain unauthorized access to a work does not take effect until the end of a two-year

⁸⁸⁶ Cunard & Coplan, “WIPO Treaty Implementation: Debate Over OSP Liability,” *Computer Law Strategist* (Oct. 1997) 1, 3.

period beginning on the date of enactment of the bill – the two year waiting period expired on October 28, 2000, and the prohibition is now in effect.

(i) Exemptions Adopted by the Librarian of Congress

Section 1201(a)(1) requires the Librarian of Congress, upon recommendation of the Register of Copyrights and in consultation with the Assistant Secretary of Commerce for Communications and Information, to conduct a rulemaking⁸⁸⁷ during the initial two-year period, and during each succeeding three-year period, to determine whether certain types of users of copyrighted works are, or are likely to be, adversely affected by the prohibition in Section 1201(a)(1).⁸⁸⁸ The Librarian must publish a list of particular classes of copyrighted works for which the rulemaking determines that noninfringing uses have been, or are likely to be, adversely affected, and the prohibitions of Section 1201(a) shall not apply to such users with respect to such class of works for the ensuing three-year period.

The Exemptions of 2000. On Oct. 27, 2000, the Copyright Office published the first set of classes of copyrighted works that the Librarian of Congress determined would be exempt from the anti-circumvention provisions of Section 1201(a)(1), with the exemption to be in effect until Oct. 28, 2003.⁸⁸⁹ Those classes, which were only two in number and very narrowly defined, were as follows:

1. Compilations consisting of lists of websites blocked by filtering software and applications. The Librarian determined that an exemption was necessary to avoid an adverse effect on persons who wish to criticize and comment on such lists, because they would not be able to ascertain which sites are on the lists unless they circumvented encryption protecting the contents of the lists.⁸⁹⁰

2. Literary works, including computer programs and databases, protected by access control mechanisms that fail to permit access because of malfunction, damage or obsolescence. The Librarian determined that an exemption was necessary to gain access to literary works

⁸⁸⁷ As originally passed by Congress, section 1201(a)(1) required that the rulemaking be on the record. However, the Intellectual Property and Communications Omnibus Reform Act of 1999, P.L. 106-113, passed by Congress on Nov. 19, 1999 and signed by the President in late 1999, removed the requirement that the rulemaking be “on the record.”

⁸⁸⁸ Section 1201(a)(C) provides that in conducting the rulemaking, the Librarian shall examine the availability for use of copyrighted works; the availability for use of works for nonprofit archival, preservation, and educational purposes; the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research; and the effect of circumvention of technological measures on the market for or value of copyrighted works.

⁸⁸⁹ 65 Fed. Reg. 64556 (Oct. 27, 2000).

⁸⁹⁰ *Id.* at 64564.

protected by access control mechanisms, such as dongles or other mechanisms, that malfunction or become obsolete.⁸⁹¹

The Exemptions of 2003. On Oct. 27, 2003, the Copyright Office issued the second determination of the classes of copyrighted works that the Librarian decided should have an exemption, with the exemption to be in effect until Oct. 27, 2006.⁸⁹² The classes, which were only four in number and even more specifically defined than the first set of classes,⁸⁹³ were as follows:

1. Compilations consisting of lists of Internet locations blocked by commercially marketed filtering software applications that are intended to prevent access to domains, websites or portions of websites, but not including lists of Internet locations blocked by software applications that operate exclusively to protect against damage to a computer or computer network or lists of Internet locations blocked by software applications that operate exclusively to prevent receipt of email.⁸⁹⁴ The Librarian defined “Internet locations” to “include domains, uniform resource locators (URLs), numeric IP addresses or any combination thereof.”⁸⁹⁵ This class is similar to the first class of exemptions in the Librarian’s first determination, but was narrowed so as to exclude the ability to circumvent blocked lists associated with firewalls, anti-virus software and anti-spam software.⁸⁹⁶

2. Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. This class is similar to the second class of exemptions in the Librarian’s first determination, but was narrowed to cover only the case of obsolete dongles because the Librarian found that this was the only class for which adequate factual support of potential harm had been submitted in the second rulemaking proceeding.⁸⁹⁷ The Librarian

⁸⁹¹ Id. at 64564-66. For the Copyright Office’s rationale for rejecting an exemption for a host of other proposed classes of works, see id. at 64566-74.

⁸⁹² 68 Fed. Reg. 62011 (Oct. 31, 2003).

⁸⁹³ A statement accompanying the Librarian’s decision with respect to the exempted classes partially explained the narrowness of the classes: “It is important to understand the purposes of this rulemaking, as stated in the law, and the role I have in it. The rulemaking is not a broad evaluation of the successes or failures of the DMCA. The purpose of the proceeding is to determine whether current technologies that control access to copyrighted works are diminishing the ability of individuals to use works in lawful, noninfringing ways. The DMCA does not forbid the act of circumventing copy controls, and therefore this rulemaking proceeding is not about technologies that control copying. Some of the people who participated in the rulemaking did not understand that and made proposals based on their dissatisfaction with copy controls. Other participants sought exemptions that would permit them to circumvent access controls on all works when they are engaging in particular noninfringing uses of those works. The law does not give me that power.” Statement of the Librarian of Congress Relating to Section 1201 Rulemaking, available as of Oct. 30, 2003 at www.copyright.gov/1201/docs/librarian_statement_01.html.

⁸⁹⁴ 68 Fed. Reg. at 62013.

⁸⁹⁵ Id.

⁸⁹⁶ Id.

⁸⁹⁷ Id. at 62013-14.

defined “obsolete” as “no longer manufactured or reasonably available in the commercial marketplace.”⁸⁹⁸

3. Computer programs and video games distributed in formats that have become obsolete and which require the original media or hardware as a condition of access. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace. The Librarian determined that this exemption is necessary to allow archiving or continued use of computer programs and video games that are subject to “original media only” restrictions, are stored on media no longer in use, such as 5.25” floppy disks, or require use of an obsolete operating system.⁸⁹⁹

4. Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling of the ebook’s read-aloud function and that prevent the enabling of screen readers to render the text into a specialized format. The Librarian defined “specialized format,” “digital text” and “authorized entities” to have the same meaning as in 17 U.S.C. § 121.⁹⁰⁰ The Librarian determined that this exemption is necessary in response to problems experienced by the blind and visually impaired in gaining meaningful access to literary works distributed as ebooks.⁹⁰¹

For the Copyright Office’s rationale for rejecting an exemption for a host of other proposed classes of works, see 68 Fed. Reg. at 62014-18. One of the more interesting proposed exemptions that the Copyright Office rejected was one submitted by Static Control Components, Inc. in response to the district court’s ruling in the case of Lexmark International, Inc. v. Static Control Components, Inc.,⁹⁰² discussed in Section II.G.1(o)(1) below. In that case, the district court ruled on a motion for a preliminary injunction that Static Control violated Section 1201(a)(2) by distributing microchips that were used to replace the microchip found in plaintiff Lexmark’s toner cartridges so as to circumvent Lexmark’s authentication sequence that prevented the printer engine software on the Lexmark printer from allowing the printer to operate with a refilled toner cartridge. In view of this ruling, Static Control submitted a proposed exemption to the Copyright Office to permit circumvention of access controls on computer programs embedded in computer printers and toner cartridges and that control the interoperation and functions of the printer and toner cartridge. The Copyright Office concluded that the statutory exemption set forth in Section 1201(f), discussed in Section II.G.1(g) below,

⁸⁹⁸ Id. at 62018.

⁸⁹⁹ Id. at 62014.

⁹⁰⁰ Id.

⁹⁰¹ Id.

⁹⁰² 253 F. Supp. 2d 943, 948-49 (E.D. Ky. 2003), rev’d, 387 F.3d 522 (6th Cir. 2004), reh’g denied, 2004 U.S. App. LEXIS 27422 (Dec. 29, 2004), reh’g en banc denied, 2005 U.S. App. LEXIS 3330 (6th Cir. Feb. 15, 2005).

already adequately addressed the concerns of toner cartridge re-manufacturers.⁹⁰³ The rationale for the Copyright Office’s conclusion is discussed further in Section II.G.1(g) below.

The Exemptions of 2006. On Nov. 27, 2006, the Copyright Office issued the third determination of the classes of copyrighted works that the Librarian decided should have an exemption, with the exemption to be in effect until Oct. 27, 2009.⁹⁰⁴ In previous rulemakings, the Copyright Office had determined that an exempted class must be based primarily on attributes of the work itself and not the nature of the use or the user. In its 2006 ruling, the Copyright Office determined for the first time that in certain circumstances it would be permissible to refine the description of a class of works by reference to the type of user who may take advantage of the exemption or by reference to the type of use of the work that may be made pursuant to the exemption, and the Copyright Office applied this refinement to some of the classes of works exempted.⁹⁰⁵

The exempted classes of works in the 2006 ruling were the following:

1. “Audiovisual works included in the educational library of a college or university’s film or media studies department, when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors.”⁹⁰⁶ This exemption was the first one to define the class by reference to particular types of uses and users.

2. “Computer programs and video games distributed in formats that have become obsolete and that require the original media or hardware as a condition of access, when circumvention is accomplished for the purpose of preservation or archival reproduction of published digital works by a library or archive. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace.”⁹⁰⁷ This exemption is the same as the third class in the 2003 ruling, except that a definition of what renders constitutes an obsolete format was added.

3. “Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer

⁹⁰³ 68 Fed. Reg. at 62017.

⁹⁰⁴ 71 Fed. Reg. 68472 (Nov. 27, 2006). On Oct. 27, 2009, the Librarian of Congress extended the 2006 exemptions on an interim basis until the Copyright Office and Librarian of Congress could complete their decision with respect to the next classes of exemptions to be granted. See 74 Fed. Reg. 55139 (Oct. 27, 2009). The extension period turned out to be 9 months, ending on July 26, 2010.

⁹⁰⁵ Id. at 68473-74.

⁹⁰⁶ Id.

⁹⁰⁷ Id. at 68474.

manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.”⁹⁰⁸ This exemption is the same as the second class in the 2003 ruling.

4. “Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book’s read-aloud function or of screen readers that render the text into a specialized format.”⁹⁰⁹ This exemption is similar to the fourth class in the 2003 ruling, except that the two requirements in the description of the access controls is phrased in the disjunctive, whereas in the 2003 ruling it was phrased in the conjunctive.

5. “Computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network.”⁹¹⁰ This is a new exemption, and is another one defined by reference to a particular type of use. The purpose of this exemption is to address the use of software locks that prevent customers from using their handsets on a competitor’s network, even after all contractual obligations to the original wireless carrier have been satisfied, by controlling access to the firmware that operates the mobile phone. The Copyright Office justified the exemption by noting that “in this case, the access controls do not appear to actually be deployed in order to protect the interests of the copyright owner or the value or integrity of the copyrighted work; rather, they are used by wireless carriers to limit the ability of subscribers to switch to other carriers, a business decision that has nothing whatsoever to do with the interests protected by copyright. ... When application of the prohibition on circumvention of access controls would offer no apparent benefit to the author or copyright owner in relation to the work to which access is controlled, but simply offers a benefit to a third party who may use § 1201 to control the use of hardware which, as is increasingly the case, may be operated in part through the use of computer software or firmware, an exemption may well be warranted.”⁹¹¹ The rationale underlying this class is an important one, and may be applied to justify more exempted classes in future rulemakings by the Copyright Office.

6. “Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.”⁹¹² This exemption was prompted by the notorious case of the DRM technology

⁹⁰⁸ Id. at 68475.

⁹⁰⁹ Id.

⁹¹⁰ Id. at 68476.

⁹¹¹ Id.

⁹¹² 71 Fed. Reg. 68477.

that Sony BMG Music added to some music CDs distributed in 2005 and that went awry, causing damage to users' computers.

Among the proposed classes that the Copyright Office rejected was the interesting one of an exemption for "space-shifting" to permit circumvention of access controls applied to audiovisual and musical works in order to copy these works to other media or devices and to access these works on those alternative media or devices. The Copyright Office rejected the proposal on the ground that those proposing the exemption "uniformly failed to cite legal precedent that establishes that such space-shifting is, in fact, a noninfringing use. The Register concludes that the reproduction of those works onto new devices is an infringement of the exclusive reproduction right unless some exemption or defense is applicable. In the absence of any persuasive legal authority for the proposition that making copies of a work onto any device of the user's choosing is a noninfringing use, there is no basis for recommending an exemption to the prohibition on circumvention."⁹¹³ The Copyright Office also rejected a proposed exemption for all works protected by access controls that prevent the creation of backup copies, reasoning that "the proponents offered no legal arguments in support of the proposition that the making of backup copies is noninfringing."⁹¹⁴

The Exemptions of 2010. On July 27, 2010, the Librarian of Congress issued the fourth determination of the classes of copyrighted works that should have an exemption, with the exemption to be in effect until Oct. 27, 2012.⁹¹⁵ The 2010 ruling continued the approach of the 2006 ruling in refining the description of a class of works by reference to the type of user who may take advantage of the exemption or by reference to the type of use of the work that may be made pursuant to the exemption. Indeed, in announcing the exemption, the Copyright Office stated that the prohibitions against circumvention "shall not apply to persons who are users of a copyrighted work which is in a particular class of works" granted an exemption.⁹¹⁶

The six exempted classes of works in the 2010 ruling are the following:

1. "Motion pictures on DVDs that are lawfully made and acquired and that are protected by the Content Scrambling System when circumvention is accomplished solely in order to accomplish the incorporation of short portions of motion pictures into new works for the purpose of criticism or comment, and where the person engaging in circumvention believes and has reasonable grounds for believing that circumvention is necessary to fulfill the purpose of the use in the following instances:

(i) Educational uses by college and university professors and by college and university film and media studies students;

⁹¹³ Id. at 68478.

⁹¹⁴ Id. at 68479.

⁹¹⁵ 75 Fed. Reg. 43825 (July 27, 2010).

⁹¹⁶ Id. at 43826.

(ii) Documentary filmmaking;

(iii) Noncommercial videos.”

2. “Computer programs that enable wireless telephone handsets to execute software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications, when they have been lawfully obtained, with computer programs on the telephone handset.”

3. “Computer programs, in the form of firmware or software, that enable used⁹¹⁷ wireless telephone handsets to connect to a wireless telecommunications network, when circumvention is initiated by the owner of the copy of the computer program solely in order to connect to a wireless telecommunications network and access to the network is authorized by the operator of the network.”

4. “Video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works, when circumvention is accomplished solely for the purpose of good faith testing for, investigating, or correcting security flaws or vulnerabilities, if:

(i) The information derived from the security testing is used primarily to promote the security of the owner or operator of a computer, computer system, or computer network; and

(ii) The information derived from the security testing is used or maintained in a manner that does not facilitate copyright infringement or a violation of applicable law.”

5. “Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.”

6. “Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book’s read-aloud function or of screen readers that render the text into a specialized format.”⁹¹⁸

The Exemptions of 2012. On Oct 26, 2012, the Librarian of Congress issued the fifth determination of the classes of copyrighted works that should have an exemption, effective as of Oct. 28, 2012.⁹¹⁹ The 2012 ruling broadened somewhat the approach of the 2010 ruling’s focus on refining the description of a class of works by reference to the type of user who may take

⁹¹⁷ The limitation of this exemption to “used” wireless telephone handsets was a narrowing of the network connection exemption granted in the 2006 rulemaking.

⁹¹⁸ 75 Fed. Reg. at 43849.

⁹¹⁹ 77 Fed. Reg. 65260 (Oct. 26, 2012).

advantage of the exemption or by reference to the type of use of the work that may be made pursuant to the exemption. For example, the Copyright Office noted in its recommendation to the Librarian of Congress the following: “While beginning with a category of works identified in Section 102, or a subcategory thereof, the description of the ‘particular class’ ordinarily will be refined with reference to other factors so that the scope of the class is proportionate to the scope of harm to noninfringing uses. For example, a class might be refined in part by reference to the medium on which the works are distributed, or to the access control measures applied to the works. The description of a class of works may also be refined, in appropriate cases, by reference to the type of user who may take advantage of the exemption or the type of use that may be made pursuant to the designation.”⁹²⁰

Notably, the Librarian omitted from the exempted classes one of the broad classes that had been granted an exemption in 2010 pertaining to computer programs for “unlocking” wireless handsets to function with alternative wireless networks. Instead, the Librarian granted a much more limited exemption that applied only to handsets acquired within 90 days after the effective date of the exemption. The principle rationale for the much more limited exemption was the following:

The Register further concluded that the record before her supported a finding that, with respect to new wireless handsets, there are ample alternatives to circumvention. That is, the marketplace has evolved such that there is now a wide array of unlocked phone options available to consumers. While it is true that not *every* wireless device is available unlocked, and wireless carriers’ unlocking policies are not free from all restrictions, the record clearly demonstrates that there is a wide range of alternatives from which consumers may choose in order to obtain an unlocked wireless phone. Thus, the Register determined that with respect to newly purchased phones, proponents had not satisfied their burden of showing adverse effects related to a technological protection measure.⁹²¹

This decision on the part of the Register proved to be the source of significant subsequent controversy. In Aug. 2014 the President signed The Unlocking Consumer Choice and Wireless Competition Act, Public Law 113-144, 128 Stat. 1751 (2014), restoring and making permanent the 2010 exemption, as well as allowing the circumvention permitted under the reinstated 2010 exemption, as well as any future exemptions to permit wireless telephone handsets or other wireless devices to connect to wireless telecommunications networks, to be performed by the owner of the handset or device, by another person at the direction of the

⁹²⁰ Id. at 65261.

⁹²¹ Id. at 65265.

owner, or by a provider of commercial mobile radio or data services to enable such owners or a family member to connect to a wireless network when authorized by the network operator.⁹²²

The six exempted classes of works in the 2012 ruling are the following:

1. “Literary works, distributed electronically, that are protected by technological measures which either prevent the enabling of read-aloud functionality or interfere with screen readers or other applications or assistive technologies in the following instances:

(i) When a copy of such a work is lawfully obtained by a blind or other person with a disability, as such a person is defined in 17 U.S.C. 121; provided, however, the rights owner is remunerated, as appropriate, for the price of the mainstream copy of the work as made available to the general public through customary channels; or

(ii) When such work is a nondramatic literary work, lawfully obtained and used by an authorized entity pursuant to 17 U.S.C. 121.”

2. “Computer programs that enable wireless telephone handsets to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the telephone handset.”

3. “Computer programs, in the form of firmware or software, that enable a wireless telephone handset originally acquired from the operator of a wireless telecommunications network or retailer no later than ninety days after the effective date of this exemption to connect to a different wireless telecommunications network, if the operator of the wireless communications networks to which the handset is locked has failed to unlock it within a reasonable period of time following a request by the owner of the wireless telephone handset, and when circumvention is initiated by the owner, an individual consumer, who is also the owner of the copy of the computer program in such wireless telephone handset, solely in order to connect to a different wireless telecommunications network, and such access to the network is authorized by the operator of the network.”

4. “Motion pictures, as defined in 17 U.S.C. 101, on DVDs that are lawfully made and acquired and that are protected by the Content Scrambling System, where the person engaging in the circumvention believes and has reasonable grounds for believing that circumvention is necessary because reasonably available alternatives, such as noncircumventing methods or using screen capture software as provided for in alternative exemptions, are not able to produce the

⁹²² “President Signs Bill Restoring Consumer Right to Unlock Mobile Handsets,” *BNA’s Patent, Trademark & Copyright Journal* (Aug. 4, 2014), available as of Aug. 5, 2014 at http://iplaw.bna.com/iprc/display/simple_doc_display.adp?fedfid=50888556&vname=ptdbulallissuesdib&jd=a0f4c7w8w2&split=0#a0f4c7w8w2. The bill does not create a statutory right for consumers to unlock phones, but merely reverses the Copyright Office’s prior regulatory decision and directs the Copyright Office to initiate a rulemaking proceeding to determine whether any wireless devices in addition to cellphones should be included in the unlocking exemption. *Id.*

level of high-quality content required to achieve the desired criticism or comment on such motion pictures, and where circumvention is undertaken solely in order to make use of short portions of the motion pictures for the purpose of criticism or comment in the following instances:

- (i) In noncommercial videos;
- (ii) In documentary films;
- (iii) In nonfiction multimedia ebooks offering film analysis; and

(iv) For educational purposes in film studies or other courses requiring close analysis of film and media excerpts, by college and university faculty, college and university students, and kindergarten through twelfth grade educators. For purposes of this exemption, ‘noncommercial videos’ includes videos created pursuant to a paid commission, provided that the commissioning entity’s use is noncommercial.”

5. “Motion pictures, as defined in 17 U.S.C. 101, that are lawfully made and acquired via online distribution services and that are protected by various technological protection measures, where the person engaging in circumvention believes and has reasonable grounds for believing that circumvention is necessary because reasonably available alternatives, such as noncircumventing methods or using screen capture software as provided for in alternative exemptions, are not able to produce the level of high-quality content required to achieve the desired criticism or comment on such motion pictures, and where circumvention is undertaken solely in order to make use of short portions of the motion pictures for the purpose of criticism or comment in the following instances:

- (i) In noncommercial videos;
- (ii) In documentary films;
- (iii) In nonfiction multimedia ebooks offering film analysis; and

(iv) For educational purposes in film studies or other courses requiring close analysis of film and media excerpts, by college and university faculty, college and university students, and kindergarten through twelfth grade educators. For purposes of this exemption, “noncommercial videos” includes videos created pursuant to a paid commission, provided that the commissioning entity’s use is noncommercial.”

6. “(i) Motion pictures, as defined in 17 U.S.C. 101, on DVDs that are lawfully made and acquired and that are protected by the Content Scrambling System, where the circumvention, if any, is undertaken using screen capture technology that is reasonably represented and offered to the public as enabling the reproduction of motion picture content after such content has been lawfully decrypted, when such representations have been reasonably relied upon by the user of such technology, when the person engaging in the circumvention believes and has reasonable grounds for believing that the circumvention is necessary to achieve the desired criticism or

comment, and where the circumvention is undertaken solely in order to make use of short portions of the motion pictures for the purpose of criticism or comment in the following instances:

(A) In noncommercial videos;

(B) In documentary films;

(C) In nonfiction multimedia ebooks offering film analysis; and

(D) For educational purposes by college and university faculty, college and university students, and kindergarten through twelfth grade educators.

(ii) For purposes of this exemption, ‘noncommercial videos’ includes videos created pursuant to a paid commission, provided that the commissioning entity’s use is noncommercial.”

7. “(i) Motion pictures, as defined in 17 U.S.C. 101, that are lawfully made and acquired via online distribution services and that are protected by various technological protection measures, where the circumvention, if any, is undertaken using screen capture technology that is reasonably represented and offered to the public as enabling the reproduction of motion picture content after such content has been lawfully decrypted, when such representations have been reasonably relied upon by the user of such technology, when the person engaging in the circumvention believes and has reasonable grounds for believing that the circumvention is necessary to achieve the desired criticism or comment, and where the circumvention is undertaken solely in order to make use of short portions of the motion pictures for the purpose of criticism or comment in the following instances:

(A) In noncommercial videos;

(B) In documentary films;

(C) In nonfiction multimedia ebooks offering film analysis; and

(D) For educational purposes by college and university faculty, college and university students, and kindergarten through twelfth grade educators.

(ii) For purposes of this exemption, ‘noncommercial videos’ includes videos created pursuant to a paid commission, provided that the commissioning entity’s use is noncommercial.”

8. “Motion pictures and other audiovisual works on DVDs that are protected by the Content Scrambling System, or that are distributed by an online service and protected by technological measures that control access to such works, when circumvention is accomplished solely to access the playhead and/or related time code information embedded in copies of such works and solely for the purpose of conducting research and development for the purpose of creating players capable of rendering visual representations of the audible portions of such works and/or audible representations or descriptions of the visual portions of such works to

enable an individual who is blind, visually impaired, deaf, or hard of hearing, and who has lawfully obtained a copy of such a work, to perceive the work; provided, however, that the resulting player does not require circumvention of technological measures to operation.”⁹²³

The Exemptions of 2015. On Oct 20, 2015, the Librarian of Congress issued the sixth determination of the classes of copyrighted works that should have an exemption, effective as of Oct. 28, 2015.⁹²⁴ The Unlocking Consumer Choice and Wireless Competition Act, Public Law 113-144, 128 Stat. 1751 (2014), directed the Librarian to consider as part of this triennial proceeding whether to extend the cellphone unlocking exemption in the statute to include any other category of wireless devices based upon the recommendation of the Register, who in turn was to consult with the Assistant Secretary. The Register recommended, and the Librarian agreed, that such exemption should be extended to other wireless devices, as noted below. The sixth triennial rulemaking continued the procedure adopted in the fifth triennial rulemaking of refining a class of exempted works by reference to the use or user in order to remedy the adverse effect of the prohibition and to limit the adverse consequences of an exemption. The Copyright Office received nearly 40,000 comments in response to its Notice of Proposed Rulemaking and held seven days of public hearings in two cities.⁹²⁵

The ten exempted classes of works in the 2015 ruling are the following:

1. “Motion pictures (including television shows and videos), as defined in 17 U.S.C. 101, where circumvention is undertaken solely in order to make use of short portions of the motion pictures for the purpose of criticism or comment in the following instances:

(i) For use in documentary filmmaking,

(A) Where the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted, or

(B) Where the motion picture is lawfully made and acquired on a DVD protected by the Content Scramble System, on a Blu-ray disc protected by the Advanced Access Control System, or via a digital transmission protected by a technological measure, and where the person engaging in circumvention reasonably believes that screen-capture software or other non-circumventing alternatives are unable to produce the required level of high-quality content;

(ii) For use in noncommercial videos (including videos produced for a paid commission if the commissioning entity’s use is noncommercial),

⁹²³ Id. at 65278-79.

⁹²⁴ 80 Fed. Reg. 65944 (Oct. 28, 2015).

⁹²⁵ Id. at 65946.

(A) Where the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted, or

(B) Where the motion picture is lawfully made and acquired on a DVD protected by the Content Scramble System, on a Blu-ray disc protected by the Advanced Access Control System, or via a digital transmission protected by a technological measure, and where the person engaging in circumvention reasonably believes that screen-capture software or other non-circumventing alternatives are unable to produce the required level of high-quality content;

(iii) For use in nonfiction multimedia e-books offering film analysis,

(A) Where the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted, or

(B) Where the motion picture is lawfully made and acquired on a DVD protected by the Content Scramble System, on a Blu-ray disc protected by the Advanced Access Control System, or via a digital transmission protected by a technological measure, and where the person engaging in circumvention reasonably believes that screen-capture software or other non-circumventing alternatives are unable to produce the required level of high-quality content;

(iv) By college and university faculty and students, for educational purposes,

(A) Where the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted, or

(B) In film studies or other courses requiring close analysis of film and media excerpts where the motion picture is lawfully made and acquired on a DVD protected by the Content Scramble System, on a Blu-ray disc protected by the Advanced Access Control System, or via a digital transmission protected by a technological measure, and where the person engaging in circumvention reasonably believes that screen-capture software or other non-circumventing alternatives are unable to produce the required level of high-quality content;

(v) By faculty of massive open online courses (MOOCs) offered by accredited nonprofit educational institutions to officially enrolled students through online platforms (which platforms themselves may be operated for profit), for educational purposes, where the MOOC provider through the online platform limits transmissions to the extent technologically feasible to such officially enrolled students, institutes copyright policies and provides copyright informational materials to faculty, students and relevant staff members, and applies technological measures that reasonably prevent unauthorized further dissemination of a work in accessible form to others or retention of the work for longer than the course session by recipients of a transmission through the platform, as contemplated by 17 U.S.C. 110(2),

(A) Where the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted, or

(B) In film studies or other courses requiring close analysis of film and media excerpts where the motion picture is lawfully made and acquired on a DVD protected by the Content Scramble System, on a Blu-ray disc protected by the Advanced Access Control System, or via a digital transmission protected by a technological measure, and where the person engaging in circumvention reasonably believes that screen-capture software or other non-circumventing alternatives are unable to produce the required level of high-quality content;

(vi) By kindergarten through twelfth-grade educators, including of accredited general educational development (GED) programs, for educational purposes,

(A) Where the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted, or

(B) In film studies or other courses requiring close analysis of film and media excerpts where the motion picture is lawfully made and acquired on a DVD protected by the Content Scramble System, or via a digital transmission protected by a technological measure, and where the person engaging in circumvention reasonably believes that screen-capture software or other non-circumventing alternatives are unable to produce the required level of high-quality content;

(vii) By kindergarten through twelfth-grade students, including those in accredited general educational development (GED) programs, for educational purposes, where the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted; and

(viii) By educators and participants in nonprofit digital and media literacy programs offered by libraries, museums and other nonprofit entities with an educational mission, in the course of face-to-face instructional activities for educational purposes, where the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted.”

2. “Literary works, distributed electronically, that are protected by technological measures that either prevent the enabling of read-aloud functionality or interfere with screen readers or other applications or assistive technologies,

(i) When a copy of such a work is lawfully obtained by a blind or other person with a disability, as such a person is defined in 17 U.S.C. 121; provided, however, that the rights owner is remunerated, as appropriate, for the price of the mainstream copy of the work as made available to the general public through customary channels, or

(ii) When such work is a nondramatic literary work, lawfully obtained and used by an authorized entity pursuant to 17 U.S.C. 121.”

3. “(i) Computer programs that enable the following types of wireless devices to connect to a wireless telecommunications network, when circumvention is undertaken solely in order to connect to a wireless telecommunications network and such connection is authorized by the operator of such network, and the device is a used device:

(A) Wireless telephone handsets (i.e., cellphones);

(B) All-purpose tablet computers;

(C) Portable mobile connectivity devices, such as mobile hotspots, removable wireless broadband modems, and similar devices; and

(D) Wearable wireless devices designed to be worn on the body, such as smartwatches or fitness devices.

(ii) A device is considered “used” for purposes of this exemption when it has previously been lawfully acquired and activated on the wireless telecommunications network of a wireless carrier.”

4. “Computer programs that enable smartphones and portable all-purpose mobile computing devices to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the smartphone or device, or to permit removal of software from the smartphone or device. For purposes of this exemption, a ‘portable all-purpose mobile computing device’ is a device that is primarily designed to run a wide variety of programs rather than for consumption of a particular type of media content, is equipped with an operating system primarily designed for mobile use, and is intended to be carried or worn by an individual.”

5. “Computer programs that enable smart televisions to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the smart television.”

6. “Computer programs that are contained in and control the functioning of a motorized land vehicle such as a personal automobile, commercial motor vehicle or mechanized agricultural vehicle, except for computer programs primarily designed for the control of telematics or entertainment systems for such vehicle, when circumvention is a necessary step undertaken by the authorized owner of the vehicle to allow the diagnosis, repair or lawful modification of a vehicle function; and where such circumvention does not constitute a violation of applicable law, including without limitation regulations promulgated by the Department of Transportation or the Environmental Protection Agency; and provided, however, that such circumvention is initiated no earlier than 12 months after the effective date of this regulation.”

7. “(i) Computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates solely for the purpose of good-faith security research and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code; and provided, however, that, except as to voting machines, such circumvention is initiated no earlier than 12 months after the effective date of this regulation, and the device or machine is one of the following:

(A) A device or machine primarily designed for use by individual consumers (including voting machines);

(B) A motorized land vehicle; or

(C) A medical device designed for whole or partial implantation in patients or a corresponding personal monitoring system, that is not and will not be used by patients or for patient care.

(ii) For purposes of this exemption, “good-faith security research” means accessing a computer program solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability, where such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.”

8. “(i) Video games in the form of computer programs embodied in physical or downloaded formats that have been lawfully acquired as complete games, when the copyright owner or its authorized representative has ceased to provide access to an external computer server necessary to facilitate an authentication process to enable local gameplay, solely for the purpose of:

(A) Permitting access to the video game to allow copying and modification of the computer program to restore access to the game for personal gameplay on a personal computer or video game console; or

(B) Permitting access to the video game to allow copying and modification of the computer program to restore access to the game on a personal computer or video game console when necessary to allow preservation of the game in a playable form by an eligible library, archives or museum, where such activities are carried out without any purpose of direct or indirect commercial advantage and the video game is not distributed or made available outside of the physical premises of the eligible library, archives or museum.

(ii) Computer programs used to operate video game consoles solely to the extent necessary for an eligible library, archives or museum to engage in the preservation activities described in paragraph (i)(B).

(iii) For purposes of the exemptions in paragraphs (i) and (ii), the following definitions shall apply:

(A) “Complete games” means video games that can be played by users without accessing or reproducing copyrightable content stored or previously stored on an external computer server.

(B) “Ceased to provide access” means that the copyright owner or its authorized representative has either issued an affirmative statement indicating that external server support for the video game has ended and such support is in fact no longer available or, alternatively, server support has been discontinued for a period of at least six months; provided, however, that server support has not since been restored.

(C) “Local gameplay” means gameplay conducted on a personal computer or video game console, or locally connected personal computers or consoles, and not through an online service or facility.

(D) A library, archives or museum is considered “eligible” when the collections of the library, archives or museum are open to the public and/or are routinely made available to researchers who are not affiliated with the library, archives or museum.”

9. “Computer programs that operate 3D printers that employ microchip-reliant technological measures to limit the use of feedstock, when circumvention is accomplished solely for the purpose of using alternative feedstock and not for the purpose of accessing design software, design files or proprietary data; provided, however, that the exemption shall not extend to any computer program on a 3D printer that produces goods or materials for use in commerce the physical production of which is subject to legal or regulatory oversight or a related certification process, or where the circumvention is otherwise unlawful.”

10. “Literary works consisting of compilations of data generated by medical devices that are wholly or partially implanted in the body or by their corresponding personal monitoring systems, where such circumvention is undertaken by a patient for the sole purpose of lawfully accessing the data generated by his or her own device or monitoring system and does not constitute a violation of applicable law, including without limitation the Health Insurance Portability and Accountability Act of 1996, the Computer Fraud and Abuse Act of 1986 or regulations of the Food and Drug Administration, and is accomplished through the passive monitoring of wireless transmissions that are already being produced by such device or monitoring system.”⁹²⁶

The Exemptions of 2018. On Oct 26, 2018, the Librarian of Congress issued the seventh determination of the classes of copyrighted works that should have an exemption.⁹²⁷ For the seventh triennial proceeding, the Copyright Office implemented a new streamlining process

⁹²⁶ *Id.* at 65961-64.

⁹²⁷ 83 Fed. Reg. 54010 (Oct. 26, 2018).

enabling members of the public to seek renewal of existing exemptions to which there was no meaningful opposition. Streamlined renewal was based upon a determination that, due to a lack of legal, marketplace, or technological changes, the factors that led the Register to recommend adoption of the exemption in the prior rulemaking are expected to continue into the forthcoming triennial period. Under this new procedure, the Copyright Office recommended, and the Librarian agreed, to the re-adoption of all exemptions granted in the 2015 rulemaking. In addition, new exemptions were approved. The seventh triennial rulemaking continued the procedure used in the two previous triennial rulemakings of refining a class of exempted works by reference to the use or user in order to remedy the adverse effect of the prohibition and to limit the adverse consequences of an exemption. The Copyright Office received 181 total submissions in response to its Notice of Proposed Rulemaking, substantially less than the nearly 40,000 comments received in response to the previous rulemaking. In analyzing the written comments, the Copyright Office held seven days of hearings in Washington D.C. (April 10-13) and Los Angeles, California (April 23-25), both of which were live streamed online.⁹²⁸

The fourteen exempted classes of works in the 2018 ruling are the following:

1. “Motion pictures (including television shows and videos), as defined in 17 U.S.C. 101, where the motion picture is lawfully made and acquired on a DVD protected by the Content Scramble System, on a Blu-ray disc protected by the Advanced Access Content System, or via a digital transmission protected by a technological measure, and the person engaging in circumvention under paragraph (b)(1)(i) and (b)(1)(ii)(A) and (B) of this section reasonably believes that non-circumventing alternatives are unable to produce the required level of high-quality content, or the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted, where circumvention is undertaken solely in order to make use of short portions of the motion pictures in the following instances:

(i) For the purpose of criticism or comment:

(A) For use in documentary filmmaking, or other films where the motion picture clip is used in parody or for its biographical or historically significant nature;

(B) For use in noncommercial videos (including videos produced for a paid commission if the commissioning entity’s use is noncommercial); or

(C) For use in nonfiction multimedia e-books.

(ii) For educational purposes:

(A) By college and university faculty and students or kindergarten through twelfth-grade (K–12) educators and students (where the K–12 student is circumventing under the direct

⁹²⁸ Id. at 54011-12.

supervision of an educator), including of accredited general educational development (GED) programs, for the purpose of criticism, comment, teaching, or scholarship;

(B) By faculty of massive open online courses (MOOCs) offered by accredited nonprofit educational institutions to officially enrolled students through online platforms (which platforms themselves may be operated for profit), in film studies or other courses requiring close analysis of film and media excerpts, for the purpose of criticism or comment, where the MOOC provider through the online platform limits transmissions to the extent technologically feasible to such officially enrolled students, institutes copyright policies and provides copyright informational materials to faculty, students, and relevant staff members, and applies technological measures that reasonably prevent unauthorized further dissemination of a work in accessible form to others or retention of the work for longer than the course session by recipients of a transmission through the platform, as contemplated by 17 U.S.C. 110(2); or

(C) By educators and participants in nonprofit digital and media literacy programs offered by libraries, museums, and other nonprofit entities with an educational mission, in the course of face-to-face instructional activities, for the purpose of criticism or comment, except that such users may only circumvent using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted.”

2. “(i) Motion pictures (including television shows and videos), as defined in 17 U.S.C. 101, where the motion picture is lawfully acquired on a DVD protected by the Content Scramble System, on a Blu-ray disc protected by the Advanced Access Content System, or via a digital transmission protected by a technological measure, where:

(A) Circumvention is undertaken by a disability services office or other unit of a kindergarten through twelfth-grade educational institution, college, or university engaged in and/or responsible for the provision of accessibility services to students, for the purpose of adding captions and/or audio description to a motion picture to create an accessible version as a necessary accommodation for a student or students with disabilities under an applicable disability law, such as the Americans With Disabilities Act, the Individuals with Disabilities Education Act, or Section 504 of the Rehabilitation Act;

(B) The educational institution unit in paragraph (b)(2)(i)(A) of this section has, after a reasonable effort, determined that an accessible version cannot be obtained at a fair price or in a timely manner; and

(C) The accessible versions are provided to students or educators and stored by the educational institution in a manner intended to reasonably prevent unauthorized further dissemination of a work.

(ii) For purposes of this paragraph (b)(2), “audio description” means an oral narration that provides an accurate rendering of the motion picture.”

3. “Literary works, distributed electronically, that are protected by technological measures that either prevent the enabling of read-aloud functionality or interfere with screen readers or other applications or assistive technologies:

(i) When a copy of such a work is lawfully obtained by a blind or other person with a disability, as such a person is defined in 17 U.S.C. 121; provided, however, that the rights owner is remunerated, as appropriate, for the price of the mainstream copy of the work as made available to the general public through customary channels; or

(ii) When such work is a nondramatic literary work, lawfully obtained and used by an authorized entity pursuant to 17 U.S.C. 121.”

4. “Literary works consisting of compilations of data generated by medical devices that are wholly or partially implanted in the body or by their corresponding personal monitoring systems, where such circumvention is undertaken by a patient for the sole purpose of lawfully accessing the data generated by his or her own device or monitoring system and does not constitute a violation of applicable law, including without limitation the Health Insurance Portability and Accountability Act of 1996, the Computer Fraud and Abuse Act of 1986 or regulations of the Food and Drug Administration, and is accomplished through the passive monitoring of wireless transmissions that are already being produced by such device or monitoring system.”

5. “Computer programs that enable the following types of lawfully acquired wireless devices to connect to a wireless telecommunications network, when circumvention is undertaken solely in order to connect to a wireless telecommunications network and such connection is authorized by the operator of such network:

(i) Wireless telephone handsets (i.e., cellphones);

(ii) All-purpose tablet computers;

(iii) Portable mobile connectivity devices, such as mobile hotspots, removable wireless broadband modems, and similar devices; and

(iv) Wearable wireless devices designed to be worn on the body, such as smartwatches or fitness devices.”

6. “Computer programs that enable smartphones and portable all-purpose mobile computing devices to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the smartphone or device, or to permit removal of software from the smartphone or device. For purposes of this paragraph (b)(6), a “portable all-purpose mobile computing device” is a device that is primarily designed to run a wide variety of programs rather than for consumption of a particular type of media content, is equipped with an operating

system primarily designed for mobile use, and is intended to be carried or worn by an individual.”

7. “Computer programs that enable smart televisions to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the smart television.”

8. “Computer programs that enable voice assistant devices to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the device, or to permit removal of software from the device, and is not accomplished for the purpose of gaining unauthorized access to other copyrighted works. For purposes of this paragraph (b)(8), a “voice assistant device” is a device that is primarily designed to run a wide variety of programs rather than for consumption of a particular type of media content, is designed to take user input primarily by voice, and is designed to be installed in a home or office.”

9. “Computer programs that are contained in and control the functioning of a lawfully acquired motorized land vehicle such as a personal automobile, commercial vehicle, or mechanized agricultural vehicle, except for programs accessed through a separate subscription service, when circumvention is a necessary step to allow the diagnosis, repair, or lawful modification of a vehicle function, where such circumvention does not constitute a violation of applicable law, including without limitation regulations promulgated by the Department of Transportation or the Environmental Protection Agency, and is not accomplished for the purpose of gaining unauthorized access to other copyrighted works.”

10. “Computer programs that are contained in and control the functioning of a lawfully acquired smartphone or home appliance or home system, such as a refrigerator, thermostat, HVAC, or electrical system, when circumvention is a necessary step to allow the diagnosis, maintenance, or repair of such a device or system, and is not accomplished for the purpose of gaining access to other copyrighted works. For purposes of this paragraph (b)(10):

(i) The “maintenance” of a device or system is the servicing of the device or system in order to make it work in accordance with its original specifications and any changes to those specifications authorized for that device or system; and

(ii) The “repair” of a device or system is the restoring of the device or system to the state of working in accordance with its original specifications and any changes to those specifications authorized for that device or system.”

11. “(i) Computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates, or is undertaken on a computer, computer system, or computer network on which the computer program operates with the authorization of the owner or operator of such computer, computer system, or computer network, solely for the purpose of good-faith security research and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986.

(ii) For purposes of this paragraph (b)(11), “good-faith security research” means accessing a computer program solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in an environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.”

12. “(i) Video games in the form of computer programs embodied in physical or downloaded formats that have been lawfully acquired as complete games, when the copyright owner or its authorized representative has ceased to provide access to an external computer server necessary to facilitate an authentication process to enable gameplay, solely for the purpose of:

(A) Permitting access to the video game to allow copying and modification of the computer program to restore access to the game for personal, local gameplay on a personal computer or video game console; or

(B) Permitting access to the video game to allow copying and modification of the computer program to restore access to the game on a personal computer or video game console when necessary to allow preservation of the game in a playable form by an eligible library, archives, or museum, where such activities are carried out without any purpose of direct or indirect commercial advantage and the video game is not distributed or made available outside of the physical premises of the eligible library, archives, or museum.

(ii) Video games in the form of computer programs embodied in physical or downloaded formats that have been lawfully acquired as complete games, that do not require access to an external computer server for gameplay, and that are no longer reasonably available in the commercial marketplace, solely for the purpose of preservation of the game in a playable form by an eligible library, archives, or museum, where such activities are carried out without any purpose of direct or indirect commercial advantage and the video game is not distributed or made available outside of the physical premises of the eligible library, archives, or museum.

(iii) Computer programs used to operate video game consoles solely to the extent necessary for an eligible library, archives, or museum to engage in the preservation activities described in paragraph (b)(12)(i)(B) or (b)(12)(ii) of this section.

(iv) For purposes of this paragraph (b)(12), the following definitions shall apply:

(A) For purposes of paragraph (b)(12)(i)(A) and (b)(12)(ii) of this section, “complete games” means video games that can be played by users without accessing or reproducing copyrightable content stored or previously stored on an external computer server.

(B) For purposes of paragraph (b)(12)(i)(B) of this section, “complete games” means video games that meet the definition in paragraph (b)(12)(iv)(A) of this section, or that consist of

both a copy of a game intended for a personal computer or video game console and a copy of the game's code that was stored or previously stored on an external computer server."

(C) "Ceased to provide access" means that the copyright owner or its authorized representative has either issued an affirmative statement indicating that external server support for the video game has ended and such support is in fact no longer available or, alternatively, server support has been discontinued for a period of at least six months; provided, however, that server support has not since been restored.

(D) "Local gameplay" means gameplay conducted on a personal computer or video game console, or locally connected personal computers or consoles, and not through an online service or facility.

(E) A library, archives, or museum is considered "eligible" when the collections of the library, archives, or museum are open to the public and/or are routinely made available to researchers who are not affiliated with the library, archives, or museum."

13. "(i) Computer programs, except video games, that have been lawfully acquired and that are no longer reasonably available in the commercial marketplace, solely for the purpose of lawful preservation of a computer program, or of digital materials dependent upon a computer program as a condition of access, by an eligible library, archives, or museum, where such activities are carried out without any purpose of direct or indirect commercial advantage and the program is not distributed or made available outside of the physical premises of the eligible library, archives, or museum.

(ii) For purposes of the exemption in paragraph (b)(13)(i) of this section, a library, archives, or museum is considered "eligible" if—

(A) The collections of the library, archives, or museum are open to the public and/or are routinely made available to researchers who are not affiliated with the library, archives, or museum;

(B) The library, archives, or museum has a public service mission;

(C) The library, archives, or museum's trained staff or volunteers provide professional services normally associated with libraries, archives, or museums;

(D) The collections of the library, archives, or museum are composed of lawfully acquired and/or licensed materials; and

(E) The library, archives, or museum implements reasonable digital security measures as appropriate for the activities permitted by this paragraph (b)(13).

14. "Computer programs that operate 3D printers that employ microchip- reliant technological measures to limit the use of feedstock, when circumvention is accomplished solely

for the purpose of using alternative feedstock and not for the purpose of accessing design software, design files, or proprietary data.”

“Persons who may initiate circumvention. To the extent authorized under paragraph (b) of this section, the circumvention of a technological measure that restricts wireless telephone handsets or other wireless devices from connecting to a wireless telecommunications network may be initiated by the owner of any such handset or other device, by another person at the direction of the owner, or by a provider of a commercial mobile radio service or a commercial mobile data service at the direction of such owner or other person, solely in order to enable such owner or a family member of such owner to connect to a wireless telecommunications network, when such connection is authorized by the operator of such network.”⁹²⁹

The Exemptions of 2021. On Oct 28, 2021, the Librarian of Congress issued the eighth determination of the classes of copyrighted works that should have an exemption.⁹³⁰ For the eighth triennial proceeding, the Copyright Office continued the streamlining process that it began in the seventh triennial proceeding enabling members of the public to seek renewal of existing exemptions upon a determination that, due to a lack of legal, marketplace, or technological changes, the factors that led the Register to recommend adoption of the exemption in the prior rulemaking are expected to continue into the forthcoming triennial period. Under the renewal procedure, the Copyright Office recommended, and the Librarian agreed, to the re-adoption of all exemptions granted in the 2018 rulemaking. The eighth triennial rulemaking continued the procedure used in the three previous triennial rulemakings of refining a class of exempted works by reference to the use or user in order to remedy the adverse effect of the prohibition and to limit the adverse consequences of an exemption. The Copyright Office received 161 total submissions in response to its Notice of Proposed Rulemaking and held seven days of public hearings on the proposed exemptions.⁹³¹

Several new exemptions or expansions were approved. Among the most notable were:

- A new exemption that allows for circumvention of technological measures on any device or machine (except a gaming console) to investigate potential violations of licenses for free and open source software. Any such investigation must be performed on a legally obtained device and not violate other laws. The investigation must also be performed by, or on behalf of, a party with standing to bring a breach of license or copyright claim that has a good faith belief that the investigation is necessary. Further, the investigation must be for the sole purpose of investigating potential infringement.

⁹²⁹ Id. at 5428-31.

⁹³⁰ 86 Fed. Reg. 59627 (Oct. 28, 2021).

⁹³¹ Id. at 59627-29.

- Another new exemption allows for circumvention of technical measures on motion pictures and literary works stored on DVDs or Blu-ray discs, or made available for digital download, for researchers to perform text and data mining. The circumvention must be applied by a researcher affiliated with a nonprofit institution, or a student or information technology staff member under such a researcher's direction, and the institution must legally own or license a copy of the copyrighted work. The work may be watched or read only for the purpose of validating the results of the research and the institution must employ effective security measures to prevent further dissemination of the work. For institutions and research projects that qualify, the exemption may provide easier access to rich sources of data for analyzing cultural phenomena and development.
- The exemptions for the right to repair software-enabled devices like video game consoles were expanded to cover all consumer devices. The Register found that diagnosis, maintenance and repair of software-enabled consumer devices are likely to be fair uses where the purpose is to restore device functionality. The eighth triennial proceeding also added an additional exemption specifically for the repair of medical devices. For video game consoles, "repair" is limited to repair or replacement of a console's optical drive and requires restoring any technological protection measures that were circumvented or disabled.

The 21 exempted classes of works in the 2021 ruling are the following:

1. "Motion pictures (including television shows and videos), as defined in 17 U.S.C. 101, where the motion picture is lawfully made and acquired on a DVD protected by the Content Scramble System, on a Blu-ray disc protected by the Advanced Access Content System, or via a digital transmission protected by a technological measure, and the person engaging in circumvention under paragraphs (b)(1)(i) and (b)(1)(ii)(A) and (B) of this section reasonably believes that non-circumventing alternatives are unable to produce the required level of high-quality content, or the circumvention is undertaken using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted, where circumvention is undertaken solely in order to make use of short portions of the motion pictures in the following instances:

(i) For the purpose of criticism or comment:

(A) For use in documentary filmmaking, or other films where the motion picture clip is used in parody or for its biographical or historically significant nature;

(B) For use in noncommercial videos (including videos produced for a paid commission if the commissioning entity's use is noncommercial); or

(C) For use in nonfiction multimedia e-books.

(ii) For educational purposes:

(A) By college and university faculty and students or kindergarten through twelfth-grade (K–12) educators and students (where the K–12 student is circumventing under the direct supervision of an educator), or employees acting at the direction of faculty of such educational institutions for the purpose of teaching a course, including of accredited general educational development (GED) programs, for the purpose of criticism, comment, teaching, or scholarship;

(B) By faculty of accredited nonprofit educational institutions and employees acting at the direction of faculty members of those institutions, for purposes of offering massive open online courses (MOOCs) to officially enrolled students through online platforms (which platforms themselves may be operated for profit), in film studies or other courses requiring close analysis of film and media excerpts, for the purpose of criticism or comment, where the MOOC provider through the online platform limits transmissions to the extent technologically feasible to such officially enrolled students, institutes copyright policies and provides copyright informational materials to faculty, students, and relevant staff members, and applies technological measures that reasonably prevent unauthorized further dissemination of a work in accessible form to others or retention of the work for longer than the course session by recipients of a transmission through the platform, as contemplated by 17 U.S.C. 110(2); or

(C) By educators and participants in nonprofit digital and media literacy programs offered by libraries, museums, and other nonprofit entities with an educational mission, in the course of face-to-face instructional activities, for the purpose of criticism or comment, except that such users may only circumvent using screen-capture technology that appears to be offered to the public as enabling the reproduction of motion pictures after content has been lawfully acquired and decrypted.”

2.

“(i) Motion pictures (including television shows and videos), as defined in 17 U.S.C. 101, where the motion picture is lawfully acquired on a DVD protected by the Content Scramble System, on a Blu-ray disc protected by the Advanced Access Content System, or via a digital transmission protected by a technological measure, where:

(A) Circumvention is undertaken by a disability services office or other unit of a kindergarten through twelfth-grade educational institution, college, or university engaged in and/or responsible for the provision of accessibility services for the purpose of adding captions and/or audio description to a motion picture to create an accessible version for students, faculty, or staff with disabilities;

(B) The educational institution unit in paragraph (b)(2)(i)(A) of this section has a reasonable belief that the motion picture will be used for a specific future activity of the institution and, after a reasonable effort, has determined that an accessible version of sufficient quality cannot be obtained at a fair market price or in a timely manner, including where a copyright holder has not provided an accessible version of a motion picture that was included with a textbook; and

(C) The accessible versions are provided to students or educators and stored by the educational institution in a manner intended to reasonably prevent unauthorized further dissemination of a work.

(ii) For purposes of paragraph (b)(2) of this section,

(A) “Audio description” means an oral narration that provides an accurate rendering of the motion picture;

(B) “Accessible version of sufficient quality” means a version that in the reasonable judgment of the educational institution unit has captions and/or audio description that are sufficient to meet the accessibility needs of students, faculty, or staff with disabilities and are substantially free of errors that would materially interfere with those needs; and

(C) Accessible materials created pursuant to this exemption and stored pursuant to paragraph (b)(2)(i)(C) of this section may be reused by the educational institution unit to meet the accessibility needs of students, faculty, or staff with disabilities pursuant to paragraphs (b)(2)(i)(A) and (B) of this section.”

3.

“(i) Motion pictures (including television shows and videos), as defined in 17 U.S.C. 101, where the motion picture is lawfully acquired on a DVD protected by the Content Scramble System, or on a Blu-ray disc protected by the Advanced Access Content System, solely for the purpose of lawful preservation or the creation of a replacement copy of the motion picture, by an eligible library, archives, or museum, where:

(A) Such activity is carried out without any purpose of direct or indirect commercial advantage;

(B) The DVD or Blu-ray disc is damaged or deteriorating;

(C) The eligible institution, after a reasonable effort, has determined that an unused and undamaged replacement copy cannot be obtained at a fair price and that no streaming service, download service, or on-demand cable and satellite service makes the motion picture available to libraries, archives, and museums at a fair price; and

(D) The preservation or replacement copies are not distributed or made available outside of the physical premises of the eligible library, archives, or museum.

(ii) For purposes of paragraph (b)(3)(i) of this section, a library, archives, or museum is considered “eligible” if—

(A) The collections of the library, archives, or museum are open to the public and/or are routinely made available to researchers who are not affiliated with the library, archives, or museum;

(B) The library, archives, or museum has a public service mission;

(C) The library, archives, or museum's trained staff or volunteers provide professional services normally associated with libraries, archives, or museums;

(D) The collections of the library, archives, or museum are composed of lawfully acquired and/or licensed materials; and

(E) The library, archives, or museum implements reasonable digital security measures as appropriate for the activities permitted by paragraph (b)(3)(i) of this section."

4.

"(i) Motion pictures, as defined in 17 U.S.C. 101, where the motion picture is on a DVD protected by the Content Scramble System, on a Blu-ray disc protected by the Advanced Access Content System, or made available for digital download where:

(A) The circumvention is undertaken by a researcher affiliated with a nonprofit institution of higher education, or by a student or information technology staff member of the institution at the direction of such researcher, solely to deploy text and data mining techniques on a corpus of motion pictures for the purpose of scholarly research and teaching;

(B) The copy of each motion picture is lawfully acquired and owned by the institution, or licensed to the institution without a time limitation on access;

(C) The person undertaking the circumvention views or listens to the contents of the motion pictures in the corpus solely for the purpose of verification of the research findings; and

(D) The institution uses effective security measures to prevent further dissemination or downloading of motion pictures in the corpus, and to limit access to only the persons identified in paragraph (b)(4)(i)(A) of this section or to researchers affiliated with other institutions of higher education solely for purposes of collaboration or replication of the research.

(ii) For purposes of paragraph (b)(4)(i) of this section:

(A) An institution of higher education is defined as one that:

(1) Admits regular students who have a certificate of graduation from a secondary school or the equivalent of such a certificate;

(2) Is legally authorized to provide a postsecondary education program;

(3) Awards a bachelor's degree or provides not less than a two-year program acceptable towards such a degree;

(4) Is a public or other nonprofit institution; and

(5) Is accredited by a nationally recognized accrediting agency or association.

(B) The term “effective security measures” means security measures that have been agreed to by interested copyright owners of motion pictures and institutions of higher education; or, in the absence of such measures, those measures that the institution uses to keep its own highly confidential information secure. If the institution uses the security measures it uses to protect its own highly confidential information, it must, upon a reasonable request from a copyright owner whose work is contained in the corpus, provide information to that copyright owner regarding the nature of such measures.”

5.

“(i) Literary works, excluding computer programs and compilations that were compiled specifically for text and data mining purposes, distributed electronically where:

(A) The circumvention is undertaken by a researcher affiliated with a nonprofit institution of higher education, or by a student or information technology staff member of the institution at the direction of such researcher, solely to deploy text and data mining techniques on a corpus of literary works for the purpose of scholarly research and teaching;

(B) The copy of each literary work is lawfully acquired and owned by the institution, or licensed to the institution without a time limitation on access;

(C) The person undertaking the circumvention views the contents of the literary works in the corpus solely for the purpose of verification of the research findings; and

(D) The institution uses effective security measures to prevent further dissemination or downloading of literary works in the corpus, and to limit access to only the persons identified in paragraph (b)(5)(i)(A) of this section or to researchers or to researchers affiliated with other institutions of higher education solely for purposes of collaboration or replication of the research.

(ii) For purposes of paragraph (b)(5)(i) of this section:

(A) An institution of higher education is defined as one that:

(1) Admits regular students who have a certificate of graduation from a secondary school or the equivalent of such a certificate;

(2) Is legally authorized to provide a postsecondary education program;

(3) Awards a bachelor’s degree or provides not less than a two-year program acceptable towards such a degree;

(4) Is a public or other nonprofit institution; and

(5) Is accredited by a nationally recognized accrediting agency or association.

(B) The term “effective security measures” means security measures that have been agreed to by interested copyright owners of literary works and institutions of higher education; or, in the absence of such measures, those measures that the institution uses to keep its own highly confidential information secure. If the institution uses the security measures it uses to protect its own highly confidential information, it must, upon a reasonable request from a copyright owner whose work is contained in the corpus, provide information to that copyright owner regarding the nature of such measures.”

6.

“(i) Literary works or previously published musical works that have been fixed in the form of text or notation, distributed electronically, that are protected by technological measures that either prevent the enabling of read-aloud functionality or interfere with screen readers or other applications or assistive technologies:

(A) When a copy or phonorecord of such a work is lawfully obtained by an eligible person, as such a person is defined in 17 U.S.C. 121; provided, however, that the rights owner is remunerated, as appropriate, for the market price of an inaccessible copy of the work as made available to the general public through customary channels; or

(B) When such a work is lawfully obtained and used by an authorized entity pursuant to 17 U.S.C. 121.

(ii) For the purposes of paragraph (b)(6)(i) of this section, a “phonorecord of such a work” does not include a sound recording of a performance of a musical work unless and only to the extent the recording is included as part of an audiobook or e-book.”

7. “Literary works consisting of compilations of data generated by medical devices or by their personal corresponding monitoring systems, where such circumvention is undertaken by or on behalf of a patient for the sole purpose of lawfully accessing data generated by a patient’s own medical device or monitoring system. Eligibility for this exemption is not a safe harbor from, or defense to, liability under other applicable laws, including without limitation the Health Insurance Portability and Accountability Act of 1996, the Computer Fraud and Abuse Act of 1986, or regulations of the Food and Drug Administration.”

8. “Computer programs that enable wireless devices to connect to a wireless telecommunications network, when circumvention is undertaken solely in order to connect to a wireless telecommunications network and such connection is authorized by the operator of such network.”

9. “Computer programs that enable smartphones and portable all-purpose mobile computing devices to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with

computer programs on the smartphone or device, or to permit removal of software from the smartphone or device. For purposes of this paragraph (b)(9), a “portable all-purpose mobile computing device” is a device that is primarily designed to run a wide variety of programs rather than for consumption of a particular type of media content, is equipped with an operating system primarily designed for mobile use, and is intended to be carried or worn by an individual.”

10. “Computer programs that enable smart televisions to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the smart television, and is not accomplished for the purpose of gaining unauthorized access to other copyrighted works. For purposes of this paragraph (b)(10), “smart televisions” includes both internet-enabled televisions, as well as devices that are physically separate from a television and whose primary purpose is to run software applications that stream authorized video from the internet for display on a screen.”

11. “Computer programs that enable voice assistant devices to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the device, or to permit removal of software from the device, and is not accomplished for the purpose of gaining unauthorized access to other copyrighted works. For purposes of this paragraph (b)(11), a “voice assistant device” is a device that is primarily designed to run a wide variety of programs rather than for consumption of a particular type of media content, is designed to take user input primarily by voice, and is designed to be installed in a home or office.”

12. “Computer programs that enable routers and dedicated network devices to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the router or dedicated network device, and is not accomplished for the purpose of gaining unauthorized access to other copyrighted works. For the purposes of this paragraph (b)(12), “dedicated network device” includes switches, hubs, bridges, gateways, modems, repeaters, and access points, and excludes devices that are not lawfully owned.”

13. “Computer programs that are contained in and control the functioning of a lawfully acquired motorized land vehicle or marine vessel such as a personal automobile or boat, commercial vehicle or vessel, or mechanized agricultural vehicle or vessel, except for programs accessed through a separate subscription service, when circumvention is a necessary step to allow the diagnosis, repair, or lawful modification of a vehicle or vessel function, where such circumvention is not accomplished for the purpose of gaining unauthorized access to other copyrighted works. Eligibility for this exemption is not a safe harbor from, or defense to, liability under other applicable laws, including without limitation regulations promulgated by the Department of Transportation or the Environmental Protection Agency.”

14. “Computer programs that are contained in and control the functioning of a lawfully acquired device that is primarily designed for use by consumers, when circumvention is a

necessary step to allow the diagnosis, maintenance, or repair of such a device, and is not accomplished for the purpose of gaining access to other copyrighted works. For purposes of this paragraph (b)(14):

(i) The “maintenance” of a device is the servicing of the device in order to make it work in accordance with its original specifications and any changes to those specifications authorized for that device; and

(ii) The “repair” of a device is the restoring of the device to the state of working in accordance with its original specifications and any changes to those specifications authorized for that device. For video game consoles, “repair” is limited to repair or replacement of a console’s optical drive and requires restoring any technological protection measures that were circumvented or disabled.”

15. “Computer programs that are contained in and control the functioning of a lawfully acquired medical device or system, and related data files, when circumvention is a necessary step to allow the diagnosis, maintenance, or repair of such a device or system. For purposes of this paragraph (b)(15):

(i) The “maintenance” of a device or system is the servicing of the device or system in order to make it work in accordance with its original specifications and any changes to those specifications authorized for that device or system; and

(ii) The “repair” of a device or system is the restoring of the device or system to the state of working in accordance with its original specifications and any changes to those specifications authorized for that device or system.”

16.

“(i) Computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates, or is undertaken on a computer, computer system, or computer network on which the computer program operates with the authorization of the owner or operator of such computer, computer system, or computer network, solely for the purpose of good-faith security research.

(ii) For purposes of paragraph (b)(16)(i) of this section, “good-faith security research” means accessing a computer program solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in an environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.

(iii) Good-faith security research that qualifies for the exemption under paragraph (b)(16)(i) of this section may nevertheless incur liability under other applicable laws, including

without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code, and eligibility for that exemption is not a safe harbor from, or defense to, liability under other applicable laws.”

17.

“(i) Video games in the form of computer programs embodied in physical or downloaded formats that have been lawfully acquired as complete games, when the copyright owner or its authorized representative has ceased to provide access to an external computer server necessary to facilitate an authentication process to enable gameplay, solely for the purpose of:

(A) Permitting access to the video game to allow copying and modification of the computer program to restore access to the game for personal, local gameplay on a personal computer or video game console; or

(B) Permitting access to the video game to allow copying and modification of the computer program to restore access to the game on a personal computer or video game console when necessary to allow preservation of the game in a playable form by an eligible library, archives, or museum, where such activities are carried out without any purpose of direct or indirect commercial advantage and the video game is not distributed or made available outside of the physical premises of the eligible library, archives, or museum.

(ii) Video games in the form of computer programs embodied in physical or downloaded formats that have been lawfully acquired as complete games, that do not require access to an external computer server for gameplay, and that are no longer reasonably available in the commercial marketplace, solely for the purpose of preservation of the game in a playable form by an eligible library, archives, or museum, where such activities are carried out without any purpose of direct or indirect commercial advantage and the video game is not distributed or made available outside of the physical premises of the eligible library, archives, or museum.

(iii) Computer programs used to operate video game consoles solely to the extent necessary for an eligible library, archives, or museum to engage in the preservation activities described in paragraph (b)(17)(i)(B) or (b)(17)(ii) of this section.

(iv) For purposes of this paragraph (b)(17), the following definitions shall apply:

(A) For purposes of paragraphs (b)(17)(i)(A) and (b)(17)(ii) of this section, “complete games” means video games that can be played by users without accessing or reproducing copyrightable content stored or previously stored on an external computer server.

(B) For purposes of paragraph (b)(17)(i)(B) of this section, “complete games” means video games that meet the definition in paragraph (b)(17)(iv)(A) of this section, or that consist of both a copy of a game intended for a personal computer or video game console and a copy of the game’s code that was stored or previously stored on an external computer server.

(C) “Ceased to provide access” means that the copyright owner or its authorized representative has either issued an affirmative statement indicating that external server support for the video game has ended and such support is in fact no longer available or, alternatively, server support has been discontinued for a period of at least six months; provided, however, that server support has not since been restored.

(D) “Local gameplay” means gameplay conducted on a personal computer or video game console, or locally connected personal computers or consoles, and not through an online service or facility.

(E) A library, archives, or museum is considered “eligible” if—

(1) The collections of the library, archives, or museum are open to the public and/or are routinely made available to researchers who are not affiliated with the library, archives, or museum;

(2) The library, archives, or museum has a public service mission;

(3) The library, archives, or museum’s trained staff or volunteers provide professional services normally associated with libraries, archives, or museums;

(4) The collections of the library, archives, or museum are composed of lawfully acquired and/or licensed materials; and

(5) The library, archives, or museum implements reasonable digital security measures as appropriate for the activities permitted by this paragraph (b)(17).”

18.

“(i) Computer programs, except video games, that have been lawfully acquired and that are no longer reasonably available in the commercial marketplace, solely for the purpose of lawful preservation of a computer program, or of digital materials dependent upon a computer program as a condition of access, by an eligible library, archives, or museum, where such activities are carried out without any purpose of direct or indirect commercial advantage. Any electronic distribution, display, or performance made outside of the physical premises of an eligible library, archives, or museum of works preserved under this paragraph may be made to only one user at a time, for a limited time, and only where the library, archives, or museum has no notice that the copy would be used for any purpose other than private study, scholarship, or research.

(ii) For purposes of the exemption in paragraph (b)(18)(i) of this section, a library, archives, or museum is considered “eligible” if—

(A) The collections of the library, archives, or museum are open to the public and/or are routinely made available to researchers who are not affiliated with the library, archives, or museum;

(B) The library, archives, or museum has a public service mission;

(C) The library, archives, or museum's trained staff or volunteers provide professional services normally associated with libraries, archives, or museums;

(D) The collections of the library, archives, or museum are composed of lawfully acquired and/or licensed materials; and

(E) The library, archives, or museum implements reasonable digital security measures as appropriate for the activities permitted by this paragraph (b)(18)."

19. "Computer programs that operate 3D printers that employ technological measures to limit the use of material, when circumvention is accomplished solely for the purpose of using alternative material and not for the purpose of accessing design software, design files, or proprietary data."

20. "Computer programs, solely for the purpose of investigating a potential infringement of free and open source computer programs where:

(i) The circumvention is undertaken on a lawfully acquired device or machine other than a video game console, on which the computer program operates;

(ii) The circumvention is performed by, or at the direction of, a party that has a good-faith, reasonable belief in the need for the investigation and has standing to bring a breach of license or copyright infringement claim;

(iii) Such circumvention does not constitute a violation of applicable law; and

(iv) The copy of the computer program, or the device or machine on which it operates, is not used or maintained in a manner that facilitates copyright infringement."

21. "Video games in the form of computer programs, embodied in lawfully acquired physical or downloaded formats, and operated on a general-purpose computer, where circumvention is undertaken solely for the purpose of allowing an individual with a physical disability to use software or hardware input methods other than a standard keyboard or mouse."⁹³²

a. Scope of the Network Connection Exemption – The TracFone Cases

In TracFone Wireless, Inc. v. Dixon,⁹³³ the court ruled that this exemption did not apply to the defendants' resale of unlocked TracFone phones that would work on wireless services other

⁹³² Id. at 59637-41.

⁹³³ 475 F. Supp. 2d 1236 (M.D. Fla. 2007).

than TracFone's, because the defendants' unlocking activity "was for the purpose of reselling those handsets for a profit, and not 'for the sole purpose of lawfully connecting to a wireless telephone communication network.'" ⁹³⁴ Thus, under this court's view, the exemption appears to be targeted to acts by individual owners of handsets who circumvent the phone's lock to enable their personal use of their own handset on another wireless network. It is unclear from the court's brief analysis whether the exemption would cover those who sell the "computer firmware" referenced in the exemption (and not the unlocked phone itself) that enables an individual to accomplish unlocking of his or her phone. It is also unclear whether the reference in the exemption only to "computer firmware" means that it would not apply to services rendered by a third party in assisting an individual to unlock a phone for a fee.

In TracFone Wireless, Inc. v. Riedeman, ⁹³⁵ TracFone brought claims under Section 1201 of the DMCA based on the defendant's resale of TracFone phones for which the prepaid software had been disabled. The defendant failed to file a response to the complaint and the clerk entered a default against the defendant. The court entered a judgment finding that the defendant had violated Section 1201 by circumventing technological measures that controlled access to proprietary software in the phones and by trafficking in services that circumvented technological measures protecting the software. The court also ruled that the Copyright Office exemption did not apply to the defendant's activities because the defendant's "purchase and resale of the TracFone handsets was for the purpose of reselling those handsets for a profit, and not 'for the sole purpose of lawfully connecting to a wireless telephone communication network.'" ⁹³⁶ The court entered a judgment against the defendant for statutory damages in the amount of \$1,020,800. ⁹³⁷ Interestingly, the court entered an injunction against the defendant that prohibited the defendant from even "purchasing ... any wireless mobile phone that they know or should know bears any TracFone Trademark" ⁹³⁸

In TracFone Wireless, Inc. v. GSM Group, Inc., ⁹³⁹ the defendant was engaged in bulk purchase, reflashing, and redistributing TracFone phones. The plaintiff brought claims under Section 1201 for circumvention and trafficking in circumvention technology, and the defendant moved to dismiss for failure to state a claim, relying on the Copyright Office exemption. The court denied the motion, ruling that the exemption did not apply because, citing the Dixon case, the purpose of the defendant's circumvention was to resell wireless telephone handsets for profit and not for the sole purpose of lawfully connecting to a wireless telephone communications network. ⁹⁴⁰ The court subsequently entered final judgment and a permanent

⁹³⁴ Id. at 1238.

⁹³⁵ 2007 Copyr. L. Dec. ¶ 29,500 (M.D. Fla. 2007).

⁹³⁶ Id. at p. 40,531.

⁹³⁷ Id.

⁹³⁸ Id.

⁹³⁹ 555 F. Supp. 2d 1331 (S.D. Fla. 2008).

⁹⁴⁰ Id. at 1336-37.

injunction against the defendants based on the DMCA claims on the same rationale. The permanent injunction prohibited the defendants from purchasing or selling any wireless mobile phone that the defendants knew or should have known bore any TracFone trademark and from reflashing or unlocking any such phone. The court retained jurisdiction over the matter to punish any violation of the permanent injunction in an amount of not less than \$5,000 for each TracFone handset that a defendant was found to have purchased, sold, or unlocked in violation of the injunction, or \$250,000, whichever was greater.⁹⁴¹

Similarly, in TracFone Wireless, Inc. v. Bitcell Corp.,⁹⁴² the court found the defendant's unlocking and resale of TracFone phones to constitute a violation of Section 1201. The court noted that TracFone phones were sold subject to terms and conditions restricting use and sale of the phones that were set forth in printed inserts included in the packaging with the phones, were available to the public on TracFone's web site, and were referenced in printed warnings placed on the outside of the retail packaging of the phones.⁹⁴³ With no legal analysis, the court simply stated that the "Terms and Conditions and language on the packaging constitute a valid binding contract."⁹⁴⁴ The court ruled that the Copyright Office exemption did not apply because the defendant's conduct "was for the purpose of reselling those Phones for a profit, and not 'for the sole purpose of lawfully connecting to a wireless telephone communication network.'"⁹⁴⁵ As in the Riedeman case, the court entered an injunction against the defendant that prohibited the defendant from even "purchasing ... any wireless mobile phone that they know or should know bears any Registered TracFone Trademark"⁹⁴⁶ The court ruled that any violation of the injunction would be subject to a finding of contempt and a payment of liquated damages to TracFone of the greater of \$250,000 or \$5,000 for each TracFone handset purchased, sold, unlocked, altered in any way, or shipped.⁹⁴⁷

In a virtually identical opinion under similar facts, in TracFone Wireless, Inc. v. Anadisk LLC,⁹⁴⁸ the same court found a violation of Section 1201, imposed the maximum statutory damages award of \$2,500 per phone on 4,990 phones for a total award of \$12,375,000, and entered a similar injunction. The court ruled that any violation of the injunction would be subject to a finding of contempt and a payment of liquated damages to TracFone of the greater

⁹⁴¹ TracFone Wireless, Inc. v. GSM Groups, Inc., No. 07-23166-C1V Martinez-Brown, slip op. at 4-6 (S.D. Fla. Aug. 15, 2008).

⁹⁴² 2008 U.S. Dist. LEXIS 41955 (S.D. Fla. May 28, 2008).

⁹⁴³ Id. at *3.

⁹⁴⁴ Id.

⁹⁴⁵ Id. at *8.

⁹⁴⁶ Id. at *9.

⁹⁴⁷ Id. at *12.

⁹⁴⁸ 685 F. Supp. 2d 1304 (S.D. Fla. 2010).

of \$1,000,000 or \$5,000 for each TracFone handset purchased, sold, unlocked, altered in any way, or shipped.⁹⁴⁹

And again in TracFone Wireless, Inc. v. SND Cellular, Inc., the same court imposed the maximum statutory damages award of \$11,370,000 based on trafficking in a minimum of 4,548 phones and entered a similar injunction. Again the court ruled that any violation of the injunction would be subject to a finding of contempt and a payment of liquated damages to TracFone of the greater of \$1,000,000 or \$5,000 for each TracFone handset purchased, sold, unlocked, re-flashed, altered in any way, or shipped.⁹⁵⁰

In TracFone Wireless, Inc. v. Zip Wireless Products, Inc.,⁹⁵¹ the court denied a motion to dismiss TracFone's claims of copyright infringement on the ground that the Copyright Office exemption applied. TracFone had adequately alleged in its complaint that lawful connection to a wireless telephone network was not the sole purpose of the defendants' circumvention efforts, and that factual allegation was sufficient to overcome the defendants' argument that TracFone's DMCA claims fell within the scope of the exemption.⁹⁵²

In TracFone Wireless, Inc. v. Bequator Corp., the court rejected the applicability of the Copyright Office's July 2010 exemption to the defendant's bulk resale of unlocked or reflashed TracFone phones. The court noted that the July 2010 exemption applied only to used wireless telephone handsets and therefore did not cover the defendant's activities. The court granted a maximum statutory damages award of \$46,540,000 (\$2500 per phone sold) and entered a permanent injunction against the defendants. Any violation of the injunction would incur liquidated damages in the amount of the greater of \$1,000,000 or \$5,000 for each TracFone handset purchased, sold, unlocked, reflashed, altered, rekitted, advertised, solicited and/or shipped in violation of the injunction.⁹⁵³

(ii) Epic Games v. Altmeyer

In this case, the court issued a TRO enjoining the defendant from offering services to modify Microsoft's Xbox 360 to play pirated copies of the plaintiff's video game *Gears of War 2*. The Xbox contained the capability to allow users to play the game live online, and to do so, players were required to connect through an official web site. The software involved in playing live was programmed to detect modifications to the Xbox and to recognize pirated games. If modification or piracy was detected, the user would be banned from playing live. The defendant offered a service to modify the Xbox to that neither the system itself nor the live software could recognize pirated games or any modification. The court found a likelihood of establishing that

⁹⁴⁹ Id. at 1317-18 & 1319-20.

⁹⁵⁰ TracFone Wireless, Inc. v. SND Cellular, Inc., 715 F. Supp. 2d 1246, 1263-64 (S.D. Fla. 2010).

⁹⁵¹ 716 F. Supp. 2d 1275 (N.D. Ga. 2010).

⁹⁵² Id. at 1285.

⁹⁵³ TracFone Wireless, Inc. v. Bequator Corp., 2011 U.S. Dist. LEXIS 42314 at *32-35, *41-44 (S.D. Fla. Apr. 13, 2011).

the offered services violated Section 1201(a)(2), and issued a TRO enjoining the defendant from performing, advertising, marketing, distributing, or selling game console modification services.⁹⁵⁴

(iii) Facebook v. Power Ventures

In this case, the defendants operated an Internet service called Power.com that collected user information from Facebook's web site outside of the "Facebook Connect" application programmer's interface (API). After a user provided his or her user names and passwords, the Power.com service used the access information to scrape user data from those accounts. Facebook's Terms of Use broadly prohibited the downloading, scraping, or distributing of any content on the web site, except that a user was permitted to download his or her own user content. Facebook alleged that it had implemented specific technical measures to block access by Power.com after the defendants informed Facebook that they intended to continue their service without using Facebook Connect, and that the defendants then attempted to circumvent those technological measures in violation of the anti-circumvention provisions of the DMCA. The defendants brought a motion to dismiss the DMCA claims, arguing that the unauthorized use requirement of a Section 1201(a)(1) claim was not met because it was the users who were controlling access (via Power.com) to their own content on the Facebook web site. The court denied the motion, in view of the fact that the defendants' argument relied on an assumption that Facebook users were authorized to use Power.com or similar services to access their user accounts, and the Terms of Use barred users from using automated programs to access the Facebook web site.⁹⁵⁵

(iv) Bose v. Zavala

In this case, the defendant sold Bose Lifestyle Media Centers in auctions on eBay. In his auctions, he offered to unlock the region coding within the Media Center's DVD player by altering Bose's firmware in the device or to give the purchaser directions on how to do so. Unlocking the region code would permit the Media Centers to play DVDs distributed anywhere in the world. Bose brought claims against the defendant under Section 1201 of the DMCA and the defendant moved to dismiss them under Fed. R. Civ. Pro. 12(b)(6) on the ground that Bose lacked standing to assert the claims because it was not the type of party protected by the DMCA, since it did not sell digital media or region code-changing services. The court rejected this argument, ruling that a party who controls the technological measures that protect copyrighted works is a "person injured" by the circumvention of the measures within the meaning of Section 1203(c).⁹⁵⁶ The court concluded, "Bose controls region coding, a technological measure that protects copyrighted DVDs. This is sufficient to allege that it is a 'person injured' within the meaning of the DMCA."

⁹⁵⁴ Epic Games, Inc. v. Altmeyer, 2008 U.S. Dist. LEXIS 89758 at * 3-4, *9-10 & *19 (S.D. Ill. Nov. 5, 2008).

⁹⁵⁵ Facebook, Inc. v. Power Ventures, Inc., 2009 U.S. Dist. LEXIS 42367 at *1-2, *9-10 & *13-14 (N.D. Cal. May 11, 2009).

⁹⁵⁶ Bose BV v. Zavala, 2010 U.S. Dist. LEXIS 2719 at *1-5 (D. Mass. Jan. 14, 2010).

(v) MGE UPS Systems v. GE

In MGE UPS Systems Inc. v. GE Consumer & Industrial Inc.,⁹⁵⁷ the Fifth Circuit ruled that mere use of a copyrighted work subsequent to an illegal circumvention does not violate Section 1201(a). The plaintiff distributed uninterruptible power supplies (UPS's), some of which required the use of MGE's copyrighted software programs during servicing. The software required connection of a security dongle to a laptop serial port during servicing. Software hackers had published information on the Internet disclosing general instructions on how to defeat the external security features of the dongle, thereby rendering the hacked software accessible for use without limitation. The defendant's employees obtained a hacked copy of MGE's software and used it to service the plaintiff's UPS's. The Fifth dismissed the plaintiff's claim that such use violated Section 1201(a). The court ruled that because Section 1201(a)(1) is targeted at circumvention, it does not apply to the use of copyrighted works after the technological measure has been circumvented. There was no evidence showing that a representative or employee of the defendant had altered the software such that a dongle was not required to use it, and hence the defendant had not itself engaged in any circumvention.⁹⁵⁸

(vi) Granger v. One Call Lender Services

In this case, the plaintiff was the owner of a computer program that estimated the rate or cost of real estate title insurance sold by title insurance agents. The defendants placed an infringing version of the rate calculator program on their website, though later took it down upon receipt of a demand letter from the plaintiff. The plaintiffs had embedded within the computer program copyright tag lines and a watermark that, if not removed carefully, could leave a tell-tale sign as to the origin of the work. The plaintiff argued that removal of the watermark constituted circumvention in violation of Section 1201 and sought statutory damages. The court rejected this argument, citing authority that in the Third Circuit, the legal theory of circumvention had been applied solely to circumstances where the conduct complained of entailed circumventing protective measures such as passwords, server software, or other technological barriers, as opposed to the embedded copyright tag lines and watermark at issue in the present case. Accordingly, the plaintiff could not recover damages for circumvention, although it could recover damages for removal of CMI.⁹⁵⁹

(vii) Dish Network v. World Cable

In Dish Network L.L.C. v. World Cable Inc.,⁹⁶⁰ plaintiffs Dish Network and EchoStar Technologies brought claims under Sections 1201(a)(1)(A) and 1201(a)(2) against a group of defendants in connection with the unauthorized distribution of Dish Network signals through the defendants' World Cable network. Dish Network utilized a "conditional access system" to

⁹⁵⁷ 622 F.3d 361 (5th Cir. 2010).

⁹⁵⁸ Id. at 364-66.

⁹⁵⁹ Granger v. One Call Lender Services, LLC, 2012 U.S. Dist. LEXIS 104885 at *2-4, *14-15 (E.D. Pa. July 26, 2012).

⁹⁶⁰ 893 F. Supp. 2d 452 (E.D.N.Y. 2012).

provide security for its satellite signals, which was comprised of digitally compressing and encrypting the signals, transmitting the encrypted signals to satellites and back down to a customer's satellite dish antenna, then relaying by a cable wire to the customer's EchoStar receiver that contained a smart card that functioned with the receiver to decrypt the signal if the customer was authorized to view the signal. Dish Network entered into subscription agreements with several of the individual defendants, who were undisclosed agents or employees of World Cable, that authorized the defendants to view Dish Network programming only at the address associated with their particular account and that prohibited them from rebroadcasting or transmitting the Dish Network signals. Based on an undercover investigation, Dish Network discovered that the EchoStar receivers associated with the individual accounts were not located at the addresses associated with the accounts and Dish Network signals decoded by those receivers were being routed from the individual accounts and rebroadcast through the World Cable distribution system. The defendants brought a motion to dismiss the DMCA claims and in response Dish Network brought a motion to file a second amended complaint to strengthen its DMCA claims. The court's opinion addressed both motions together, concluding that, even with the proposed amendments to the complaint, the plaintiffs could not plausibly allege Section 1201 violations. The court therefore granted the defendants' motion to dismiss and denied the plaintiffs' motion to amend the DMCA claims.⁹⁶¹

Turning first to the Section 1201(a)(1)(A) claim, the court began by noting that the plaintiffs were not alleging that the defendants used or sold a pirate access device to circumvent the conditional access system, but rather that the defendants used their EchoStar receivers as part of the World Cable rebroadcasting scheme to circumvent the conditional access system. In opposition to the motion to dismiss, the plaintiffs argued that the rebroadcasting scheme enabled World Cable subscribers to avoid or bypass the plaintiffs' encryption which should have protected those signals. In support of their motion to amend, the plaintiffs took a completely different position, arguing that the defendants themselves circumvented the encryption mechanism through fraud and deceit by misrepresenting that they intended to use their Dish Network accounts solely for residential or commercial viewing of the subject channels at the specific locations identified in their subscription agreements.⁹⁶²

The court rejected both arguments. With respect to the first one, the court held that the defendants could not be liable under Section 1201(a)(1)(A) for any alleged circumvention by the World Cable subscribers, but rather only for circumventions that they themselves performed. With respect to the second argument, the court ruled that using deception to gain access to copyrighted material is not the type of circumvention that Congress intended to combat in passing the DMCA. Here, while the defendants' alleged fraud may have circumvented *contractual* barriers to receiving the signal, there were no facts in the first amended complaint from which the court could infer that they circumvented any digital walls that protected the copyrighted works. Nor was there a basis from which the court could infer that simply moving the EchoStar receiver to an unauthorized location avoided or bypassed a digital wall, as opposed

⁹⁶¹ Id. at 456-57, 462-68.

⁹⁶² Id. at 463-64.

to a contractual restriction. The plaintiffs attempted to rectify this deficiency in the proposed second amended complaint by adding an allegation that the EchoStar receivers associated with the defendants' individual accounts were fully integrated into the World Cable system, where they were then used in real-time to decrypt signals to the World Cable subscribers, thus circumventing the plaintiffs' encryption by, among other things, bypassing or removing Dish Network's encryption that should have protected the signals. The court noted, however, that the plaintiffs did not allege that being fully integrated into the World Cable system altered or interfered with the normal process by which the EchoStar receiver and smart card decrypted the signal. At most, the plaintiffs had alleged that, by integrating the EchoStar receivers into the World Cable system, the defendants were able to effectuate a more seamless rebroadcasting of the decrypted signal. But the court noted that, under Second Circuit law, the DMCA does not concern itself with the use of protected materials after circumvention has occurred.⁹⁶³

The court further noted that, even assuming the use of deception to obtain the EchoStar receivers meant that the defendants' *use* of those receivers to decrypt the signals was without permission, it did not necessarily follow that the defendants' *access* to the decrypted signals was unauthorized. The court cited several cases for the proposition that, in the context of the DMCA, "authorized" access means the use of the normal process or the intended mechanism for obtaining the copyrighted work. The use of the words "avoid" and "bypass" in the statute, as well as the remainder of the words describing circumvention, imply that a person circumvents a technological measure only when he affirmatively performs an action that disables or voids the measure that was installed to prevent him from accessing the copyrighted material. Thus, even assuming that the defendants gained access to the Dish Network signals through fraud and deceit, the defendants' use of the normal process to decrypt the satellite signal did not avoid or bypass the conditional access system because they used the intended mechanism – the EchoStar receiver and smart card – in precisely the manner in which they were designed to function. Accordingly, the court ruled that the plaintiffs had failed to plausibly allege in both the first amended complaint and the proposed second amended complaint that the defendants violated Section 1201(a)(1)(A), and therefore granted the defendants' motion to dismiss and denied the plaintiffs' motion to amend with respect to that claim.⁹⁶⁴

Turning to the plaintiffs' anti-trafficking claim under Section 1201(a)(2) based on the defendants' distribution of the World Cable boxes, the court noted there was no dispute that the World Cable boxes did not actually decrypt the Dish Network signals. The court cited legislative history of the DMCA in which Congress made clear that the devices targeted under Section 1201(a)(2) were not those that facilitate the distribution of unlawfully received copyrighted material, but rather those devices or services that actually perform the circumvention. Accordingly, the court concluded the plaintiffs had failed to allege any facts from which the court could infer that the World Cable service or the World Cable boxes actually enabled the World Cable subscribers to circumvent the Dish Network conditional access system. The court

⁹⁶³ *Id.* at 464-65.

⁹⁶⁴ *Id.* at 465-66.

therefore granted the defendants' motion to dismiss and denied the plaintiffs' motion to amend with respect to the Section 1201(a)(2) claim.⁹⁶⁵

(viii) Eyepartner v. Kor Media Group

In Eyepartner, Inc. v. Kor Media Group LLC,⁹⁶⁶ the plaintiff licensed the defendant its software under a limited license to use the software but not to modify or access the encrypted source code. The license agreement expressly prohibited any acts to modify, translate, reverse engineer, decompile, disassemble or create derivative works of the software. The defendants were unhappy with the quality of the software and, rather than pay for the additional application programming interface service that might have addressed the defendants' concerns, they chose to make their own modifications to the plaintiff's code by decrypting and disassembling the source code. The defendants argued that it was a fair use to disassemble the source code so that it could be modified to make the program function as they wished. The court ruled, however, that such a defense could absolve liability only as to willful copyright infringement but not as to the plaintiff's claims for violation of the anti-circumvention provisions. The court further concluded that, in any event, fair use was inappropriate because the defendants had contractually waived their rights to modify the code. The plaintiffs had used an encrypting technology called IonCube to prevent the defendants from accessing the source code of the software, which the defendants had circumvented using a "deZender" program. The court found that such acts violated Section 1201(a)(3)(A) of the DMCA and issued a preliminary injunction against the defendants.⁹⁶⁷

(ix) Granger v. Dethlefs

The plaintiff in this case created a computer program, the Pennsylvania Title Insurance Rate Calculator, designed to calculate or estimate the cost of real estate title insurance in the State of Pennsylvania. The defendants placed an allegedly infringing version of the Rate Calculator on a web page. The plaintiff asserted violations of both the anti-circumvention provisions and the integrity of copyright management information provisions of the DMCA. The court granted the defendants' motion to dismiss both claims on the predicate ground that, to establish a claim under Sections 1201 and 1202, a plaintiff must show that the material he claims is circumvented is copyrighted. Here, the plaintiff had not done so. In a previous litigation, the plaintiff had been unable to establish that he had independently created the JavaScript source code for the Rate Calculator and therefore owned a copyright in the Rate Calculator. The court in the present case found that the plaintiff was bound by that earlier ruling under the doctrine of issue preclusion. Accordingly, the plaintiff could not prove that the defendants violated the DMCA because where there is not enough evidence to show copyright ownership, it cannot be proved that any copyrighted material was altered or removed. The plaintiff's circumvention of

⁹⁶⁵ Id. at 466-68.

⁹⁶⁶ 2013 U.S. Dist. LEXIS 98370 (S.D. Fla. July 15, 2013).

⁹⁶⁷ Id. at *1-23.

copyright protection and integrity of copyright management information claims were therefore barred.⁹⁶⁸

(x) D&J Optical v. Wallace

The plaintiff in this case, operator of optical centers in Arkansas, alleged that the defendants formed a competitor, Enterprise Optical, to the plaintiff's business and, without authorization, accessed the plaintiff's computer systems and downloaded patient contact information. Among other things, the plaintiff asserted claims under Section 1201. The defendants argued that the plaintiff lacked standing to bring a lawsuit under the DMCA because it was not the owner of the copyright in the misappropriated information. The court noted that, although the Eleventh Circuit had not addressed standing under the DMCA, courts outside the Eleventh Circuit had generally held that ownership of a copyright is not necessarily a requirement to bring suit under Sections 1201 and 1203. However, the key question in the present case was whether the plaintiff's allegations indicated that the defendants circumvented a technological measure that controlled access to a protected work under the Copyright Act.⁹⁶⁹

The plaintiff asserted that the defendants wrongly circumvented the plaintiff's technological measures by installing new hardware and software on the plaintiff's "Panacea" computer system and by creating new user credentials to allow access to the plaintiff's computer system. The plaintiff argued that it had sufficiently alleged a violation of the DMCA because Panacea owned the copyright to its software program. The Panacea software stored basic demographic and contact information for each patient, as well as brief descriptions of the diagnosis, treatment history, and billing information for each patient. In the complaint, the plaintiff alleged that the defendants accessed its computer system to gain access to patient information, including the names and addresses of patients. There was no indication, however, that this type of information was a protected work under the Copyright Act. The court therefore concluded that the plaintiff had failed to allege a plausible claim for relief under Section 1201, and therefore granted the defendants' motion to dismiss that claim.⁹⁷⁰

(xi) NNG v. AVA Enterprises

The plaintiff NNG in this case owned copyrighted navigation software used in entertainment hardware for automobiles. NNG employed certain procedures to protect the software from unauthorized use. An approved licensee would be authorized to download the software and a customized "license pool," which the licensee then unlocked with a unique authentication code provided by NNG. One specific section of code in the software was specifically designed to read the authentication code and verify the authenticity of the installed software. The defendant AVA manufactured and distributed aftermarket hardware for vehicle dashboards, often including navigation software, which NNG alleged contained pirated versions

⁹⁶⁸ Granger v. Dethlefs, 2014 U.S. Dist. LEXIS 76055 at *1-3, *10-18 & *21-22 (E.D. Penn. June 2, 2014).

⁹⁶⁹ D&J Optical, Inc. v. Wallace, 2015 U.S. Dist. LEXIS 41387 at *5-7, *15-16 (M.D. Ala. Mar. 31, 2015).

⁹⁷⁰ Id. at *16-18.

of NNG's navigation software. The pirated version allegedly lacked the authentication code, thus allowing an unlimited number of devices to utilize NNG's software. NNG alleged that AVA or its agent developed code that overrode or circumvented NNG's authentication code.⁹⁷¹

AVA moved to dismiss NNG's claims under Sections 1201(a)(1), 1201(a)(2), and 1201(b). The court ruled that NNG had properly pled claims under Section 1201(a)(1) because it alleged that AVA or its agent had illegally circumvented NNG's technological protection measures that controlled access to its copyrighted software by developing code that allowed the software to run on non-approved devices. AVA argued that the authentication code merely confirmed whether the software was being run on an authorized device and did not control access to the underlying software files or code. AVA contended that NNG asserted copyright protection only in its software code, which was not protected by the license-checking procedure, and did not assert copyright protection over the experience of running the software. Stated differently, the court observed, AVA was arguing that NNG's authentication code controlled only access to the navigation software's dynamic non-literal elements (i.e., the real time experience and operation of the software), and since NNG brought only copyright infringement claims for the literal elements (the code) and individual non-literal elements (such as discrete visual and audible components), the authentication code did not effectively control access. In short, AVA argued that the technological measure must control access to the elements of the work underlying the copyright infringement cause of action in order to state a claim under Section 1201(a)(1).⁹⁷²

The court rejected these arguments, noting that AVA's position would be correct in other Circuits, but not in the Ninth Circuit in view of MDY Industries,⁹⁷³ in which the Ninth Circuit explained that a DMCA circumvention claim under Section 1201(a) creates a new anti-circumvention right distinct from the traditional exclusive rights of a copyright owner. There is thus no requirement that the circumvention lead to infringement because Section 1201(a) merely prohibits circumvention itself. MDY Industries explicitly rejected the rule from the Federal Circuit which required a plaintiff bringing a claim under Section 1201(a) to demonstrate a nexus to infringement. The court ruled that AVA's arguments were therefore foreclosed by MDY Industries. It was undisputed that the technological measure in this case, the authentication code, effectively controlled access to one element of NNG's copyrighted computer software – the dynamic non-literal elements. The fact that AVA did not allegedly infringe on copyrighted dynamic non-literal elements was therefore of no consequence, because Section 1201(a) prohibits circumvention itself. Here, the authentication code prohibited an unauthorized user from accessing the dynamic non-literal elements of NNG's navigation software, and NNG alleged that AVA bypassed that measure by removing the authentication code from the pirated software installed in the infringing units. While the dynamic non-literal elements might be irrelevant in every other claim in the case, that did not mean that NNG failed

⁹⁷¹ NNG, Kft. v. AVA Enterprises, Inc., 2015 U.S. Dist. LEXIS 88742 at *2-3 (C.D. Cal. July 8, 2015).

⁹⁷² Id. at *7-10.

⁹⁷³ MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928 (9th Cir. 2010), opinion amended and superseded on denial of reh'g, 2011 U.S. App. LEXIS 3427 (9th Cir. Feb. 17, 2011).

to state a claim under Section 1201(a)(1)(A). Therefore, NNG had properly stated a claim under that section.⁹⁷⁴

AVA challenged NNG's Section 1201(a)(2) trafficking claim on the ground that Section 1201(a)(2) applies only to devices that actually perform the circumvention, and the complaint failed to allege that the infringing units themselves did so. The court agreed with AVA. Here, AVA's infringing units were not primarily designed to circumvent any technological measure and did not conduct the actual circumvention. Rather, the infringing units merely housed the alleged pirated software to which access had already been obtained. NNG argued in response that AVA had developed a piece of code that was embedded in NNG's navigation software and would override NNG's technological measures. AVA's piece of code was then allegedly trafficked when AVA sold the infringing units. The court rejected this argument, ruling that the purpose of Section 1201(a)(2) is to prevent the trafficking of devices that allow consumers to conduct the circumvention themselves. Consumers did not purchase the infringing units so that they could then circumvent NNG's navigation software, but instead purchased the infringing units to utilize the pirated software already installed. Accordingly, NNG had failed to state a claim under Section 1201(a)(2).⁹⁷⁵

Finally, with respect to NNG's Section 1201(b) claim, the court ruled that both Sections 1201(a)(2) and 1201(b) require the device in question to actually perform the circumvention, whether that be the circumvention of an access control measure or a copyright infringement protection measure. Because the infringing units were not primarily designed to circumvent – the alleged circumvention was already complete when the infringing units were shipped to the customers – NNG had also failed to state a claim under Section 1201(b).⁹⁷⁶

(xii) Ford Motor Co. v. Autel Intelligent Technology

Ford Motor Co. was the owner of the Integrated Diagnostic System (IDS) that diagnosed potential problems with Ford vehicles and guided their service and repair. The IDS contained a software component that received information from certain hardware diagnostic tools and produced diagnoses and recommended repairs based on the information it received. The IDS software contained a data compilation file that Ford protected as a trade secret through encryption and obfuscation technology. Ford alleged that the defendant created a program to circumvent Ford's security measures and access the data file without authorization, and then inserted the data file into its own vehicle diagnosis and repair product that competed with Ford's IDS. Ford asserted that it had conclusively established that the defendant copied the entire data file onto the defendant's product because that product contained identical test or dummy codes

⁹⁷⁴ NNG, 2015 U.S. Dist. LEXIS at *11.

⁹⁷⁵ Id. at *12-14.

⁹⁷⁶ Id. at * 15-16.

as Ford's IDS. Ford asserted circumvention claims under Sections 1201(a)(1) and 1201(a)(2), and the defendant moved to dismiss under Rule 12(b)(6).⁹⁷⁷

The court granted the defendant's motion to dismiss on several grounds. First, the complaint did not allege that Ford owned a copyright on its data compilation at the time when the alleged circumvention of its technological security measures took place. The complaint simply alleged that the defendant circumvented the technological security measures that protected the data compilation file. The record showed that Ford obtained a copyright registration on its data compilation on May 20, 2014, only a few months before the lawsuit was filed. The complaint was silent as to the date when the act of circumvention allegedly occurred, although the allegations appeared to suggest it happened long before May 20, 2014. The court ruled that to state a claim under Section 1201(a)(1), Ford would need to allege that the defendant circumvented Ford's technological security measures on its data compilation at a time when that data compilation was a work protected under the copyright laws.⁹⁷⁸

Second, the court noted that the Sixth Circuit had held in the Reichert case (discussed in Section II.G.1(a)(14)(iii) below) that Section 1201 requires that a plaintiff must, as part of its burden of pleading and persuasion, show that the circumvention was done for the purpose of engaging in piracy, that is, the widespread unauthorized distribution of copyrighted works. Here, Ford's complaint did not allege that the defendant circumvented its technological security measures for the purpose of engaging in piracy. Ford had therefore failed to meet its pleading burdens and its copyright circumvention claims must be dismissed. The court, however, granted Ford leave to file an amended complaint.⁹⁷⁹

Ford then amended its complaint and the defendant again filed a motion to dismiss Ford's circumvention claims. The court ruled that Ford's amended complaint still did not adequately plead a circumvention claim under Sections 1201(a)(1) and (2). Ford claimed that the IDS contained a number of data compilations, including an FFData file that contained Ford trade secrets, and that the defendant developed or used a computer program to circumvent Ford's technological security measures and access the FFData file as well as other data from the IDS. The court ruled these allegations were insufficient to state a claim because Ford did not allege that the FFData file was copyrighted. Nor did Ford allege that its copyrights on other files were contained within the FFData file. Therefore, while Ford had alleged that the defendant circumvented its technological security measures to improperly access its trade secrets in the form of the FFData file, it had not alleged that the defendant circumvented its security measures to access a copyrighted work. Accordingly, the court granted the defendant's motion to dismiss the Section 1201 claims.⁹⁸⁰

⁹⁷⁷ Ford Motor Co. v. Autel Intelligent Technology Co., 2015 U.S. Dist. LEXIS 133201 at *2-5 (E.D. Mich. Sept. 30, 2015).

⁹⁷⁸ Id. at *17-18.

⁹⁷⁹ Id. at *18-20.

⁹⁸⁰ Ford Motor Co. v. Autel US Inc., 2016 U.S. Dist. LEXIS 85875 at *1, *9-10 (E.D. Mich. July 1, 2016).

(xiii) VBConversions v. Gulf Coast Ventures

The plaintiff in this case was the owner of software that it made available for free during a trial period. The plaintiff prevented unauthorized access to its software after expiration of the trial period by requiring users to log into the software with a registration key. Users could obtain a registration key by paying a fee and returning a license agreement. The plaintiff observed several uses of a fraudulent registration key to unlock its software from a particular computer. Tracking data collected from the unauthorized uses identified the unauthorized user as an employee of the defendant. Through the unauthorized access, the employee converted a total of 187,787 lines of Visual Basic code from the plaintiff's software into 270,625 lines of C# code. The plaintiff brought claims under Section 1201(a)(1)(A) and filed a motion for default judgment. The court proceeded to determine whether the allegations in the complaint were sufficient to entitle the plaintiff to the relief requested.⁹⁸¹

The end user license agreement accompanying the software stated that users of the software could use only registration keys generated online from the plaintiff's website emailed to the licensee by the plaintiff or its third party order processing company. The license further stated that, by using the software, licensees agreed that using an illegal or fraudulent registration key to register or unlock the software made that software copy illegal and unauthorized. The court interpreted these provisions as limiting the scope of the license to use the software to only those users who obtained a valid registration key. Compliance with those contractual terms was therefore a condition precedent to the use of the software, rather than a covenant.⁹⁸²

The court ruled that the plaintiff had sufficiently alleged a violation of Section 1201(a)(A). The plaintiff had protected access to the copyrighted software by means of a technological measure in the form of a 25-digit alphanumeric registration key that restricted access to the software. The plaintiff had adequately alleged that the defendant's employees, who were acting within the course and scope of their employment with the defendant, directly circumvented the technological measure with the use of a fraudulent registration key. Therefore, the plaintiff had sufficiently alleged that the defendants' employees unlawfully circumvented the plaintiff's technological measure, and that they were doing so as agents of their employer. Noting that the defendant profited from the circumventions, the court awarded statutory damages under Section 1203(c)(3) in the amount of \$1,200 per act of circumvention, for a total of \$40,800.⁹⁸³

(xiv) General Motors v. Dorman Products

In this case, the plaintiffs alleged that the defendants violated Section 1201(A)(1)(a) by overriding security measures used in the plaintiffs' vehicle control modules in order to program those modules with unauthorized copies of the plaintiffs' copyrighted software. The court

⁹⁸¹ VBConversions LLC v. Gulf Coast Ventures, Inc., 2016 U.S. Dist. LEXIS 105760 at *4-7 (C.D. Cal. Aug. 10, 2016).

⁹⁸² Id. at *12-13.

⁹⁸³ Id. at * 15-17, *24.

granted the defendants' motion to dismiss the claim as inadequately pled. The defendants contended that the technological measures cited by the plaintiffs as having been circumvented appeared to limit access to the plaintiffs' vehicle control modules themselves and not their copyrighted software.⁹⁸⁴ In particular, the plaintiffs had pled that their "vehicle control modules ... each include a software-based lock to prevent unauthorized programming of the modules," thereby ensuring that "only authorized users can access the modules for programming and re-programming."⁹⁸⁵ The plaintiffs further pled that the defendants started with possibly unauthorized copies of the plaintiffs' copyrighted software and then were able, through their circumvention of the plaintiffs' security measures, to gain access to the plaintiffs' vehicle control modules in order to program them with unauthorized copies of the plaintiffs' software.⁹⁸⁶

The court ruled that these allegations were insufficient to state a viable claim under the DMCA. The plaintiffs had not pled that the defendants' alleged circumvention of the plaintiffs' security measures enabled the defendants to obtain copies of the plaintiffs' copyrighted works in the first instance. Rather, the plaintiffs had expressly alleged that the defendants started with copies of the copyrighted works and then loaded them onto control modules by circumventing security measures protecting access to the control modules. Because the plaintiffs had alleged that the circumvented technological measures controlled access only to the vehicle control modules, and not the copyrighted software that the plaintiffs loaded onto those modules, the claim as pled did not state a claim for relief under the DMCA. Accordingly, the court dismissed the claim with leave to amend.⁹⁸⁷

After the plaintiffs amended their complaint, the defendants filed another motion to dismiss, which the court denied. In the amended complaint, the plaintiffs alleged that they used a "Security Access" that included a software-based lock to effectively control access to (and unauthorized programming of) original software that was installed on vehicle control modules in GM vehicles, and that the lock was designed to prevent people from accessing the software contained on the module and making unauthorized copies. The plaintiffs further alleged that they believed the defendants had defeated and were defeating this security measure and accessing the software contained on the modules in order to program the modules with unauthorized copies of GM's copyrighted vehicle control software either by making an illegal copy of the software-based security key or by otherwise hacking through or circumventing the software-based lock. The plaintiffs also alleged that a Software Transfer Tool developed by the defendants circumvented GM's technological protection measure so that service technicians and

⁹⁸⁴ General Motors LLC v. Dorman Products, Inc., 2016 U.S. Dist. LEXIS 135721 at *1-2, *19-20 (E.D. Mich. Sept. 30, 2016).

⁹⁸⁵ Id. at *20.

⁹⁸⁶ Id. at *21.

⁹⁸⁷ Id. at *20-22.

other users of the tool could access, copy and transfer GM’s copyrighted software and data files contained on GM’s vehicle modules.⁹⁸⁸

The defendants sought to dismiss this claim on the grounds that the plaintiffs’ allegations involving the Software Transfer Tool essentially accused them not of illegally circumventing the technological protection measure themselves, but of creating a device that allowed others to do so. The court rejected this argument, noting that, while the allegations regarding the Software Transfer Tool also supported a separate claim of illegal trafficking made by the plaintiffs, it was not so far-fetched for the court to infer that the defendants themselves must have also circumvented GM’s technological measures at some point. Taken as true and viewed in the context of the complaint as a whole, the plaintiffs’ factual allegations therefore supported a claim that the defendants must have circumvented GM’s Security Access feature – whether during the development and distribution of the Software Transfer Tool, or prior to that, when the defendants were allegedly copying the software onto blank modules themselves. Accordingly, the court denied the defendants’ motion to dismiss.⁹⁸⁹

(xv) Disney Enterprises v. VidAngel

The District Court’s Decision

The plaintiff movie studios brought claims against VidAngel, Inc. for violation of Section 1201(a), for infringement of the plaintiffs’ exclusive rights of reproduction and public performance, and for a preliminary injunction. VidAngel offered more than 2,500 movies and television episodes for purchase on its website, including over 80 of the plaintiffs’ copyrighted works. It purchased physical copies of each of the titles in DVD format, entered each purchased DVD into an inventory management application database and assigned a unique barcode to each physical disc case. VidAngel then used a commercially available software program to decrypt a copy of each individual title to create “intermediate” files. VidAngel then tagged the files for over 80 types of potentially objectionable content. VidAngel required its customers to purchase a physical DVD containing a particular movie or television title before the customer could stream the show from VidAngel’s server. The purchase price for each DVD was \$20. Once a purchase transaction had occurred, the disc was removed from available inventory and title to the disc was transferred to that customer’s unique user ID. VidAngel typically maintained possession of the physical DVD on behalf of the purchasers, but purchasers could request that the DVD be sent to them or could retrieve it from VidAngel’s offices.⁹⁹⁰

After a customer purchased a physical DVD, the customer was shown a listing of the various types of potentially objectionable content identified in the purchased work, as well as the number of occurrences of each such type of content within the work. The user then selected

⁹⁸⁸ General Motors L.L.C. v. Dorman Prods, Inc., 2017 U.S. Dist. LEXIS 28434 at *3-4, *11-12 (E.D. Mich. Mar. 1, 2017).

⁹⁸⁹ Id. at *12-13.

⁹⁹⁰ Disney Enterprises, Inc. v. VidAngel, Inc., 224 F. Sup. 3d at 963-65 (C.D. Cal. 2016).

the types of content he or she wished to have silenced or deleted. Each user was required to apply at least one filter in order to view a video. After selecting filters, a customer was able to view a stream of the video instantaneously on any VidAngel-supported device. Once a user had viewed a stream, the user could resell the DVD back to VidAngel for a partial credit of the \$20 purchase price. The sellback price decreased \$1 per night for standard definition purchases and \$2 per night for high-definition purchases. Once a user sold the video back to VidAngel, the user's access to the title was terminated and the remaining balance was credited back to the user's VidAngel account. If the customer kept a DVD for more than 20 days, he or she could either view it through the VidAngel platform in perpetuity, sell it back for a \$1 or \$2 credit, or request that VidAngel send the DVD to the customer.⁹⁹¹

With respect to the Section 1201(a) claim, VidAngel argued that its use of a commercially available software program to allow read-access for the purpose of creating a DVD file for uploading onto a computer didn't amount to circumvention because VidAngel was decrypting DVDs only for space shifting purposes to allow them to be viewed in another way. VidAngel asserted that the practice of space shifting is legal when performed for disc purchasers who elected to have their DVD content streamed to them rather than receiving the physical discs. The court found no support for this position. The court cited previous decisions as establishing the rule that the purchase of a DVD conveys only the authority to view the DVD, not to decrypt it. VidAngel had not offered any evidence that the plaintiffs had either explicitly or implicitly authorized DVD buyers to circumvent encryption technology on the DVD in order to view the DVD on a different platform such as VidAngel's streaming service.⁹⁹² The court noted that the Librarian of Congress and the Register of Copyrights had also recently declined to adopt an exemption that would allow circumvention of access controls on lawfully made and acquired audiovisual works for the purpose of noncommercial space shifting or format shifting.⁹⁹³

VidAngel further argued that the Family Home Movie Act of 2005 (FHMA) provided an exemption for decrypting DVDs for the purpose of accessing a disk to filter audio and visual content. VidAngel asserted in particular that the FMHA rendered its circumvention lawful because the making of a decrypted copy was the necessary first step in making a lawfully

⁹⁹¹ Id. at 964-65.

⁹⁹² Id. at 967-68.

⁹⁹³ Id. at 967-68 (citing "Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies," 80 Fed. Reg. 65944 (Oct. 28, 2015) (codified at 37 C.F.R. pt. 201)). The court also rejected VidAngel's assertion that former Solicitor General Don Verilli, while supposedly representing both the major record labels and movie studios in the Grokster case at the Supreme Court, had assured the Supreme Court that his clients agreed that space shifting is legal. The court noted that in fact Verilli had specifically stated only that his clients, the "record companies," had for some time said that it is perfectly lawful to take a CD that one has purchased and upload it onto his or her computer or iPod. The court noted that Verilli's statement did not involve movie studios, nor did it address space shifting in the context of copying DVDs. Id. at 967 n.3.

purchased DVD capable of being filtered.⁹⁹⁴ The FMHA created an exemption for copyright infringement for:

the making imperceptible, by or at the direction of a member of a private household, of limited portions of audio or video content of a motion picture, during a performance in or transmitted to that household for private home viewing, *from an authorized copy of the motion picture*, or the creation or provision of a computer program or other technology that enables such making imperceptible and that is designed and marketed to be used, at the direction of a member of a private household, for such making imperceptible, *if no fixed copy of the altered version of the motion picture is created by such computer program or other technology*.⁹⁹⁵

The court rejected this argument, noting that neither the plain language nor the legislative history of the FHMA supported VidAngel's position. Senator Orin Hatch, who introduced the FHMA to the U.S. Senate, specifically stated that the FHMA did not provide an exemption from the anti-circumvention provisions of Section 1201. He further stated that it would not be a defense to a claim of violation of Section 1201 that the circumvention was for the purpose of engaging in the conduct covered by the new exemption in the FHMA. Accordingly, the court concluded that the plaintiffs had shown a strong likelihood of success on the merits of their claim that VidAngel had violated Section 1201(a)(1)(A) by circumventing technological measures that controlled access to the plaintiffs' copyrighted works on DVDs.⁹⁹⁶

The court then turned to the plaintiffs' claims for infringement of their reproduction and public performance rights. VidAngel contended that the copies of the plaintiffs' works it made were only intermediate copies and not "copies" as defined by the Copyright Act. After decrypting into an intermediate file, VidAngel tagged the files for over 80 types of content, broke them into approximately 1,300 fragments that contained no more than 10 seconds of content, then encrypted those fragments and stored them in a secure, access-controlled location in its cloud. VidAngel asserted that the fragments were not capable of being watched until VidAngel software assembled the segments in sequence, and for each segment decrypted the content, displayed it and then discarded the segment. VidAngel insisted that case law draws a distinction between unlawful copies, which can be viewed by consumers, and lawful intermediate copies, which cannot be viewed. The court rejected this argument, noting that, although VidAngel's fragmented copies might not be able to be perceived directly by consumers, they were able to be perceived with the aid of VidAngel's software, and that was sufficient to bring VidAngel's copying within the category of acts proscribed by the statute.⁹⁹⁷

⁹⁹⁴ Id. at 968.

⁹⁹⁵ 17 U.S.C. § 110(11) (emphasis added).

⁹⁹⁶ VidAngel, 224 F. Supp. 3d at 968.

⁹⁹⁷ Id. at 969-70.

With respect to the plaintiffs' claim for infringement of their public performance rights, VidAngel argued that its service did not engage in public performances because it streamed filtered versions of motion pictures created at the direction of and owned by its customers, citing the Supreme Court's focus in the Aereo decision on whether viewers were acting as owners or possessors of the relevant product in determining whether a performance was a "public" one. The court rejected this argument. Assuming *arguendo* that VidAngel's buy/sellback service created a valid ownership interest in a DVD, such ownership would apply only to the physical DVD, not the digital content that VidAngel streamed to paying customers. Customers viewed a stream from a master copy stored on a server, not a DVD temporarily owned by the user. In addition, lawful ownership of a DVD conveyed only authorization to view the DVD, not to decrypt it for the purpose of viewing it on an alternative platform. Therefore, the court held, VidAngel's customers were not lawful owners or possessors of the digital content streamed via VidAngel's service. The plaintiffs had therefore established a strong likelihood of success on the merits of their claim that VidAngel's streaming service infringed the plaintiff's public performance rights.⁹⁹⁸

The court ruled that the FMHA did not provide VidAngel a defense to the plaintiffs' copyright infringement claims. VidAngel asserted that the FMHA expressly provides that a third party may filter and transmit content as specified by a lawful owner of a copy so long as a fixed copy of the altered content is not created. The court rejected this assertion, noting that the statute clearly requires that a performance or transmission of filtered content must come from an "authorized copy" of the motion picture. The digital content that VidAngel streamed to its customers was not from an authorized copy, but rather from a digital copy that it acquired by circumventing technological protection measures on the plaintiffs' DVDs in violation of Section 1201(a). The court also concluded that the requirement that the filtered content come from an authorized copy is a clear indication the FHMA was not intended to displace a copyright holder's exclusive reproduction right under the copyright statute.⁹⁹⁹

Finally, the court rejected VidAngel's fair use defense, principally for the reasons that VidAngel was profiting from the use of the plaintiffs' works; the essential storyline, cinematography, and acting portrayals (which were the heart of the movies) remain unchanged in the copies streamed; and the fact that a customer survey by VidAngel showing that over 51% of VidAngel customers would not watch their offerings without filtering, also meant that 49% of VidAngel's customers did not consider VidAngel's service an effective substitute for the plaintiffs' unfiltered works, such that the service was merely a superseding use for those customers. The court therefore granted the plaintiffs' request for a preliminary injunction.¹⁰⁰⁰

⁹⁹⁸ Id. at 970-71. The court also rejected VidAngel's interpretation of Aereo as supposedly holding that the public performance right is not infringed when the user pays for something other than the transmission of copyrighted works. The court noted that the Supreme Court expressly stated that it had not considered that issue. Id. at 971.

⁹⁹⁹ Id. at 971-72.

¹⁰⁰⁰ Id. at 972-74, 979.

The Ninth Circuit's Decision

On appeal, the Ninth Circuit affirmed the preliminary injunction. With respect to the plaintiffs' likelihood of success on the merits, the court quickly determined that the district court did not abuse its discretion in concluding that VidAngel's making of copies of the plaintiffs' works onto its servers by ripping DVDs infringed the plaintiffs' exclusive reproduction right. The court therefore turned to analysis of VidAngel's asserted defenses under the FHMA and fair use.¹⁰⁰¹

The court first looked to the language of the FHMA, noting that the immunity afforded under Section 110(11) for the creation or provision of a computer program or other technology that enables making imperceptible (filtering) limited portions of audio or video content of a motion picture expressly requires that the filtering be accomplished "from an authorized copy of the motion picture." VidAngel argued that it satisfied this requirement because it *began* its filtering process with an authorized copy – a lawfully purchased DVD – so that any subsequent filtered stream was also "from" that authorized copy. The court rejected this argument, noting that it would alter the statutory language of "from" to "beginning from" or "indirectly from." The court noted that Section 110(11) is headed "Exemption of certain performances and displays," indicating that the FHMA excepts compliant filtered performances, rather than the processes that make such performances possible. It further observed that the legislative history stated the FHMA was created to protect intellectual property rights, and Section 110(11) provides that nothing in the paragraph shall be construed to imply further rights under Section 106, or to have any effect on defenses or limitations on rights granted under any other section of the copyright statute. The court noted that VidAngel's interpretation of the statute – which would permit unlawful decryption and copying prior to filtering – would not preserve protection of intellectual property rights and would have effect on the existing copyright scheme.¹⁰⁰²

More importantly, the Ninth Circuit concluded that VidAngel's interpretation would create a giant loophole in copyright law, sanctioning infringement so long as it filtered some content and a copy of the work was lawfully purchased at some point. That would severely erode the commercial value of the public performance right in the digital context, permitting, for example, unlicensed streams that filter out only a movie's credits.¹⁰⁰³

The court also observed that the FHMA's sponsor, Sen. Hatch, had identified "the Clear Play Model" as one intended to be protected by the FHMA. Clear Play sold a fast-forwarding device that used video time codes to permit customers to skip specific scenes or mute specific audio. It did not make copies of the films because the time codes were integrated into the disc's encrypted content and players licensed to decrypt and play the content. So the Ninth Circuit found it unsurprising that the only other court to construe the FHMA had held that Clear Play's technology was consistent with the statutory definition, but that a filtering technology that made

¹⁰⁰¹ Disney Enterprises, Inc. v. VidAngel, Inc., 869 F.3d 848, 856-57 (9th Cir. 2017).

¹⁰⁰² Id. at 857-59.

¹⁰⁰³ Id. at 859.

digital copies from lawfully purchased discs and then filtered them, as VidAngel did, was not.¹⁰⁰⁴ Accordingly, the Ninth Circuit concluded that the district court did not abuse its discretion in concluding that VidAngel was unlikely to succeed on the merits of its FHMA defense.¹⁰⁰⁵

The Ninth Circuit also determined that the district court had correctly rejected VidAngel's fair use defense. Under the first factor, although removing objectionable content might permit a viewer to enjoy a film, it was not necessarily transformative. Under the fourth factor, VidAngel argued that its service actually benefitted the plaintiffs because it purchased discs and expanded the audience for the copyrighted works to viewers who would not watch without filtering. But the district court had found that VidAngel's service was an effective substitute for the plaintiffs' unfiltered works because surveys suggested that 49% of its customers would watch the movies without filters. The Ninth Circuit ruled that finding was not clearly erroneous.¹⁰⁰⁶

Finally, the Ninth Circuit rejected VidAngel's argument that its service was a paradigmatic example of fair use in the form of space shifting. The Ninth Circuit noted that the reported decisions had unanimously rejected the view that space shifting is fair use (although all the cases cited by the court involved situations in which space shifting was not performed by the consumer himself).¹⁰⁰⁷ The court also noted that in declining to adopt an exemption to the anti-circumvention provisions of the DMCA for space shifting, the Librarian of Congress relied on the Register of Copyright's conclusion that the law of fair use, as it stood in 2015, did not sanction broad-based space shifting or format shifting.¹⁰⁰⁸ And even assuming space shifting could be fair use, the court observed that VidAngel's service was not personal and non-commercial space shifting – it made illegal copies of pre-selected movies and then sold streams with altered content and in a different format than that in which they were purchased.¹⁰⁰⁹

Lastly, the court turned to the district court's circumvention rulings. VidAngel first argued that, like all lawful purchasers, it was authorized by the plaintiffs to decrypt the technological protection measures on the DVDs it bought. The court rejected this argument, citing its 2011 holding that Section 1201(a)(3)(A) exempts from circumvention liability only those whom a copyright owner authorizes to circumvent an *access control measure*, not those whom a copyright owner authorizes to access the *work*.¹⁰¹⁰ Section 1201(a)(3)(A) therefore does not

¹⁰⁰⁴ *Id.* at 859-60 (citing Clean Flicks of Colo., LLC v. Soderbergh, 433 F. Supp. 2d 1236, 1238, 1240 (D. Colo. 2006)).

¹⁰⁰⁵ VidAngel, 869 F.3d at 860.

¹⁰⁰⁶ *Id.* at 860-61.

¹⁰⁰⁷ *Id.* at 862 (citing A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1019 (9th Cir. 2001); UMG Recordings, Inc. v. MP3.com, Inc., 92 F. Supp. 2d 349, 351 (S.D.N.Y. 2000)).

¹⁰⁰⁸ VidAngel, 869 F.3d at 862 (citing *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, 80 Fed. Reg. 65944-01, 65960 (Oct. 28, 2015)).

¹⁰⁰⁹ VidAngel, 869 F.3d at 862.

¹⁰¹⁰ *Id.* at 863 (citing MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 953 n.16 (9th Cir. 2011)). The MDY court acknowledged a circuit split between the Second Circuit and the Federal Circuit regarding the meaning of the phrase "without the authority of the copyright owner," but chose to follow the Second Circuit's approach.

provide an exemption to circumvent to those merely having authority to *view* a DVD. Rather, lawful purchasers have permission only to view their purchased discs with a DVD or Blu-ray player licensed to decrypt the discs. Therefore, VidAngel’s “authorization to circumvent” argument failed.¹⁰¹¹

VidAngel also argued, for the first time on appeal, that the technological protection measures on the plaintiffs’ discs were use controls under Section 1201(b) rather than access controls under Section 1201(a), and therefore it could not be liable for circumvention, since Section 1201(b) does not prohibit circumvention of use controls. The court ruled that, even assuming VidAngel had not waived this argument, it failed. VidAngel contended that because the plaintiffs objected only to decryption to copy – a use of the copyrighted work – but permitted those who purchased discs to decrypt to view – a way of accessing the work – the technological protection measures were conditional access controls that should be treated as use controls governed by Section 1201(b). The court rejected this argument, noting that the statute does not provide that a technological protection measure cannot serve as both an access control and a use control.¹⁰¹² The court also cited a previous Ninth Circuit decision ruling that a technological protection measure could both control access and protect against copyright infringement, and a ruling by the Copyright Office acknowledging that the drafters of Section 1201(a) might have anticipated that DVD encryption could be both an access control and a copy control.¹⁰¹³

In sum, because VidAngel decrypted the access controls on the plaintiffs’ discs without authorization, the district court did not abuse its discretion in finding the plaintiffs likely to succeed on their Section 1201(a)(1)(A) circumvention claim. The court also concluded that the district court had not abused its discretion in finding irreparable harm, balancing the equities of the parties and considering the public interest, and therefore affirmed the granting of the preliminary injunction.¹⁰¹⁴

The District Court’s Decision Upon Remand

Upon remand the plaintiffs moved for summary judgment on liability as to four works they said were representative of all works in issue, which the court granted. With respect to the Section 1201 claim, VidAngel admitted that the protection measures the plaintiffs used – CSS, AACS and BD+ – were encryption access controls under the DMCA. VidAngel argued that because it used third party decryption software, rather than writing its own, it was like any other person who legitimately views a work using an authorized disc player, and that the third party is responsible for deciding to use unauthorized decryption. The court rejected these arguments, noting that VidAngel did not claim that the third party software it used (AnyDVD HD) to

¹⁰¹¹ VidAngel, 869 F.3d at 863.

¹⁰¹² Id. at 863-64.

¹⁰¹³ Id. at 864-65 (citing MDY, 629 F.3d at 946 and *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, 65 Fed. Reg. 64-556-01, 64,568 (Oct. 27, 200)).

¹⁰¹⁴ VidAngel, 869 F.3d 865-67.

circumvent the plaintiffs' technological protection measures was authorized by the plaintiffs or the licensing organizations of CSS, AACS and BD+ to access the works. Only authorized players could get the keys to the disc's contents, and VidAngel was never given authorized keys. The court found VidAngel's argument that it only temporarily removed the encryption on the discs, and that the contents of the discs were not changed, was a distinction without a difference, as the DMCA prohibits circumvention of technological protection measures, conduct that VidAngel expressly admitted it engaged in. Accordingly, the plaintiffs had established a violation of the DMCA.¹⁰¹⁵

With respect to the plaintiffs' copyright infringement claims, the court found it undisputed that VidAngel copied the works at issue. The undisputed facts showed that VidAngel employees made intermediate copies of the files from the discs to permit the contents to be tagged. The intermediate copies were first stored in local caches and then VidAngel made a single encrypted copy in storage. These acts constituted copying. With respect to the public performance claim, the court found it undisputed that VidAngel publicly performed the works. The court noted that at the preliminary injunction stage, VidAngel argued that its streaming service was just a private performance because its customers owned the discs and therefore those customers had the right to have the content of those discs streamed to them. The court rejected that argument on the ground that VidAngel was streaming from a master copy from its server, not from a disc actually owned by the customer. VidAngel again raised this argument on summary judgment and the court again rejected it, as VidAngel had presented no evidence to support its argument.¹⁰¹⁶

With respect to VidAngel's assertion of the Family Movie Act as a defense, the court noted that VidAngel sought to avoid the Ninth Circuit's ruling that the FMA did not apply because VidAngel was not streaming from an authorized copy of the plaintiffs' motion pictures, by asserting that new facts compelled a different outcome. VidAngel argued that its master file was created directly from an authorized copy – a disc – so its service was therefore protected. The district court noted that the Ninth Circuit rejected this argument, observing that virtually all piracy of movies originates in some way from a legitimate copy, and that VidAngel streamed not from an authorized copy, but from the master file it created by ripping the movies from discs after circumventing their technological protection measures. Because VidAngel could not deny that it streamed from its ripped master files, the district court held that the Ninth Circuit's ruling foreclosed VidAngel's defense under the FMA.¹⁰¹⁷

Finally, the district court rejected VidAngel's assertion of the fair use defense. The court first ruled that the fair use defense does not apply to circumvention claims under the DMCA, because Section 107 of the copyright statute states that certain uses of a work are not copyright infringement in violation of Sections 106 and 106A, whereas the prohibition of circumvention is in Section 1201. In addition, the court held that the fair use defense did not justify the use

¹⁰¹⁵ Disney Enterprises v. VidAngel, Inc., 371 F. Supp. 3d 708, 714-15 (C.D. Cal. 2019).

¹⁰¹⁶ Id. at 716-18.

¹⁰¹⁷ Id. at 719.

VidAngel was making of the plaintiffs' works. VidAngel sought to avoid the district court's first ruling that all the fair use factors weighed against fair use and that VidAngel was not likely to succeed on the defense, and the Ninth Circuit's affirmation of that ruling, by arguing that certain "historical facts" were in dispute that rendered summary judgment inappropriate. The court found the historical facts asserted by VidAngel – the history and origin of VidAngel's master file and whether VidAngel's access to copyrighted material was authorized – were in fact not in dispute, as VidAngel had pointed to no evidence raising any material issue as to either fact.¹⁰¹⁸

In any event, the court ruled that VidAngel's defense failed under the four fair use factors. Under the first factor, VidAngel's use was commercial in nature, which is presumptively unfair. VidAngel argued that the first factor weighed in its favor because it paid the customary price when it purchased the discs for the rights it exercised. But the court noted that when VidAngel purchased the discs, it acquired the right to view the works thereon using an authorized player, and VidAngel was not using an authorized player. In addition, VidAngel's use was not transformative. Although VidAngel pointed to its tagging of 80 types of contents and its making of 1300 fragments stored in the course of streaming as transformative, the court noted it had failed to explain how those back-office processes established that the streamed content was transformed. It remained undisputed that the content VidAngel streamed to its customers did not add anything to the works, but rather simply omitted portions that viewers found objectionable.¹⁰¹⁹

VidAngel conceded that the second factor weighed against fair use. With respect to the third factor, VidAngel did not genuinely dispute that it copied the works in their entirety, that its filtered streams omitted only portions of the works, and that the heart of the works remained unchanged. With respect to the fourth factor, VidAngel reasserted its claim that its service did not harm and actually benefitted the plaintiffs because VidAngel gave the plaintiffs their "cut" and its service increased the market for their content. The district court noted that the Ninth Circuit rejected this line of argument, holding that VidAngel's purchases of discs did not excuse its infringement. The district court also noted that, when none of the other three factors favored fair use, the market harm factor was less important. Finally, the court considered VidAngel's alternative argument that social criticism is a form of fair use, and there were triable issues as to whether VidAngel's offering was a protected form of social criticism and whether VidAngel's offering had socially significant value as free speech under the First Amendment. The court rejected these arguments, noting that VidAngel failed entirely to describe what it was criticizing and failed to present any meaningful legal analysis that would tend to show that its streaming service was a form of social criticism protected by fair use. Accordingly, the court

¹⁰¹⁸ *Id.* at 715, 720. The court also rejected VidAngel's defense that its circumvention conduct was protected by the First Amendment because it circumvented in order to pursue its "expressive interests and to build a community of like-minded subscribers." The court noted that Section 1201(a) regulates conduct (the circumvention of technological protection measures) and not expression (the use to which a person puts protected works), so Section 1201 does not tread on expressive or associative rights. *Id.* at 715-16.

¹⁰¹⁹ *Id.* at 720-21.

granted the plaintiffs' motion for summary judgment and found VidAngel liable for circumvention in violation of the DMCA and for copyright infringement.¹⁰²⁰

The Jury Trial and Permanent Injunction

At trial, a jury found that VidAngel willfully infringed the copyrights of nearly 820 films owned by the plaintiffs and awarded a little more than \$61 million in statutory damages, plus an additional \$1 million in damages for violating the DMCA when VidAngel used illegal software to bypass anti-piracy measures and rip the films off of DVDs.¹⁰²¹ In September 2019, the district court entered a permanent injunction barring VidAngel from streaming "any copyrighted works" belonging to the plaintiffs and from circumventing the digital encryption the plaintiffs put on their films.¹⁰²²

(xvi) Synopsys v. Ubiquiti Networks

In this case, Synopsys brought claims alleging that the defendants fraudulently gained access to an evaluation copy of Synopsys' copyrighted software and related support materials and then used the license keys for that evaluation copy, as well as counterfeit keys, to repeatedly and illegally access and copy the software and materials over the course of three years. Synopsys brought claims under Sections 1201(a)(1), 1201(a)(2) and 1201(b). The defendants filed a motion to dismiss the Section 1201(a)(2) and 1201(b) claims, which required the court to construe the scope of those sections and the adequacy of Synopsys' pleadings under them.¹⁰²³

Among other things, the defendants argued that Synopsys' pleadings were inadequate to state a claim because "mere use" of unauthorized keys does not violate Sections 1201(a)(2) or (b). The court rejected this argument, noting that Synopsys had alleged the defendants had been using counterfeit keys obtained *and/or created* with tools obtained through hacker web sites to circumvent Synopsys' license key system, not just mere use of counterfeit keys obtained from a third party web site. The court also agreed with Synopsys' argument that with respect to allegations of illegal manufacture and import, there was no need to show that the circumvention technology was made available to any third parties; the alleged unilateral actions of the defendant Ubiquiti in manufacturing the keys using software secured from hacker web sites and importing those keys from Taiwan into the United States were sufficient. Finally, as to the manufacture claims, the court rejected Ubiquiti's argument that human readable alphanumeric text elements like the keys at issue are not items that are "manufactured." The court noted that

¹⁰²⁰ Id. at 721-22.

¹⁰²¹ Lauren Berg, "VidAngel Owes Studios \$62M for Pirating Flicks, Jury Says," *Law360* (June 17, 2019), available as of June 17, 2019 at www.law360.com/ip/articles/1169888/.

¹⁰²² Ryan Boysen, "VidAngel Banned From Streaming Cleaned-Up Disney Movies," *Law360* (Sept. 6, 2019), available as of Sept. 9, 2019 at www.law360.com/ip/articles/1196121/.

¹⁰²³ Synopsys, Inc. v. Ubiquiti Networks, Inc., 2017 U.S. Dist. LEXIS 130070 at *2, *17 (N.D. Cal. Aug. 15, 2017). The motion to dismiss did not include the Section 1201(a)(1) claim for use of counterfeit and illicit license keys to circumvent restricted access to copyrighted materials. Id. at *21 n.4.

Ubiquiti had cited no case law in support of this novel argument, which would seem to cut a wide swath away from the protections of the DMCA.¹⁰²⁴

Ubiquiti also argued that because Section 1201(b) prevents circumvention of technological measures that are in place to protect a copyright owner, to state a claim under that section Synopsys was required to allege that its anti-circumvention technology prevented infringement, but had failed to do so because Synopsys' allegations were that its license keys merely controlled access to its software. The court rejected this argument, noting Synopsys' argument that when software is run on a machine, a copy is made in RAM and that such copying, if without permission of the owner, constitutes infringement. Synopsys contended that, by preventing its software from executing on a machine without a valid key, its key system prevented that sort of RAM copying and, therefore, prevented infringement. The court found those allegations sufficient. The court therefore denied the defendants' motion to dismiss.¹⁰²⁵

(xvii) Digital Drilling Data Sys. v. Petrolink Servs.

In this case, the plaintiff was a provider of software known as the DataLogger, which was capable of measuring and providing drilling companies and well operators with accurate and real-time data during drilling operations to steer drill bits into specific targets thousands of feet underground. The defendant, a competitor, was developing a real-time drilling data visualization program, for which it needed the data stored in the plaintiff's program. To obtain such data, the defendant developed a hacking program to break into the database of the plaintiff's program and make copies of the data in real time. The plaintiff brought anti-circumvention claims against the plaintiff under Section 1201(a)(1)(A).¹⁰²⁶

To run the DataLogger software, the user was required to insert a dongle into the USB port of the computer, which provided access to the "Interface Process" of the software by which data was inputted and outputted. In addition, the "Database Process" of the software that generated and stored the data was protected by a password. The typical user of the software did not access the Database Process directly, but rather via the Interface Process. The plaintiff contended that access to DataLogger and the Database Process was protected by three technological measures. The first protection measure was an "obfuscation architecture" under which the only point of entry was via the Interface Process, which required insertion of the dongle. The second protection measure was the dongle itself, which could be obtained only by purchasing a license to DataLogger and was embedded with a key corresponding to the DataLogger programming code. The third protection measure was the internal password protection mechanism that controlled entry into the Database Process. The password was not

¹⁰²⁴ Id. at *22-24.

¹⁰²⁵ Id. at *26-27.

¹⁰²⁶ Digital Drilling Data Sys. v. Petrolink Servs., 2018 U.S. Dist. LEXIS 83158 at *4 & *9-10 (S.D. Tex. May 17, 2018), aff'd in part, rev'd in part on other grounds and remanded, 2020 U.S. App. LEXIS 2803 (5th Cir. July 2, 2020).

intended to be entered by users, but rather was an internal mechanism designed to be used only by the program itself. The password was embedded within the software.¹⁰²⁷

To develop its hacking program, the defendant obtained a laptop running the DataLogger software from one of the plaintiff's customers, with the customer's permission. The laptop included the protection dongle. Using that computer, the defendant was able to access the database and discovered that the internal password protecting the Database Process was a default password that had not been changed. After gaining access to the Database Process, the defendant developed its own hacking program, which it installed on computers running DataLogger so that the defendant could have access to the drilling data in real time. The hack accessed the database using the internal password and periodically copied information from the database for use in its own visualization program. The plaintiff contended that each time the hack sent a query to the database, it circumvented the obfuscation architecture by avoiding or bypassing the Interface Process, circumvented the dongle by avoiding or bypassing it, and circumvented the password lock by applying a key guessed by "brute force" from a program other than the Interface Process.¹⁰²⁸

The court rejected these arguments. According to the undisputed facts, once the defendant learned that the data it sought was stored on a database hosted by vendor Firebird, the defendant discovered through online research that there was a default username and password through which Firebird databases could be accessed. The defendant tested the default login credentials, and because the plaintiff had not updated its username and password, the defendant was able to obtain access. Though such access was unauthorized by the plaintiff, it did not constitute circumvention as defined by the DMCA. The court noted many decisions holding that using the correct username and password to access a copyrighted work, even without authorization to do so, does not constitute circumvention under Section 1201(a). The court disagreed with the plaintiff's argument that the way the defendant guessed the password could be classified as a "brute force attack" prohibited by the DMCA, because the password had not been guessed at random until the right one was found. Here, the defendant simply entered the commonly-known Firebird default credentials and was granted access to the Firebird database.¹⁰²⁹

The court further held that the obfuscation architecture was not circumvented and did not control access to the Firebird database. On the contrary, it was established and known that the DataLogger data files were stored in the Firebird shared library which could be accessed independently from the DataLogger software. Because the copied files were accessible via the Firebird database without requiring interaction with the obfuscation architecture, it was neither circumvented in violation of the DMCA nor did it effectively control access to the work copied. Similarly, while the dongle might control access to the DataLogger software, it did not control access to the Firebird database where the DataLogger data was stored. The Firebird database

¹⁰²⁷ Id. at *40-41.

¹⁰²⁸ Id. at *41-43.

¹⁰²⁹ Id. at *43-44.

software was separate from the DataLogger software and did not rely on the dongle to allow access to it. The court therefore ruled that the dongle was neither circumvented by the hacker software nor did it effectively control access to the data copied. Accordingly, the court granted the defendant's motion for partial summary judgment on the anti-circumvention claims.¹⁰³⁰

On appeal the Fifth Circuit affirmed summary judgment on the DMCA claims on the basis that the USB dongle and Interface Process did not effectively control access to the database schema. The court noted that while the USB dongle and Interface Process may have effectively restricted certain unauthorized uses of the DataLogger software – for example, by preventing other companies from duplicating and running the program on laptops at other drilling sites without purchasing additional licenses – those security measure did not effectively control, and indeed were not designed to control, access to the protected database schema, as evidenced by the plaintiff's public acknowledgment that the data was stored in an open source database file to allow users to query the database using off-the-shelf products. The database, including its schema, was protected only by an internal-facing password, and the plaintiff did not appeal the district court's holding that the defendant did not circumvent that measure when it employed the commonly-known database default credentials.¹⁰³¹

(xviii) Eclipse Gaming v. Antonucci

In this case, the defendant Antonucci was the CTO of the plaintiff Eclipse Gaming Systems (EGS). Antonucci requested a buyout of his membership interest in EGS. After the parties failed to reach an agreement, Antonucci allegedly retaliated by installing a time bomb into a software application that his company, Digital Dynamics Software, Inc. (DDS) licensed to EGS for use in its machines. Antonucci alleged that he had not installed a time bomb, but rather a license check made necessary because EGS failed to pay royalties for use of DDS. In DDS's view, by virtue of the failure to pay royalties, the software EGS was running was unlicensed, so DDS installed an update that would confirm the current license or lock the program on the machines. To avoid putting its entire business in jeopardy, EGS elected to restore and use a previously-licensed and older version of DDS.¹⁰³²

DDS alleged that EGS circumvented the license verification mechanism it installed to protect its software when EGS removed the current software and installed the older version onto its machines, in violation of Section 1201(a)(1). EGS brought a motion to dismiss the Section 1201(a)(1) claim under Rule 12(b)(6). The court denied the motion, ruling that in removing DDS's new software that contained the license check and replacing it with an older version that did not, EGS employed a work-around to bypass the security measure. That EGS removed the entire new version of the software and not just the technological measure was a distinction without a difference that disregarded the factual allegations that added up to an end-run around the system. The court noted EGS had no way to go through the license check and

¹⁰³⁰ Id. at *45-47.

¹⁰³¹ Digital Drilling Data Sys. v. Petrolink Servs., 2020 U.S. App. LEXIS 20802 at *18-19, *21 (5th Cir. July 2, 2020).

¹⁰³² Eclipse Gaming Sys. v. Antonucci, 2019 U.S. Dist. LEXIS 15078 at *1-2 (N.D. Ill. Jan. 31, 2019).

access the current software absent removing it entirely. The court therefore found that EGS's acts were analogous to circumventing the deployed technological measure in the measure's gatekeeping capacity by uprooting the locked gate. Accordingly, DDS had stated a claim under the DMCA and the court denied EGS's motion to dismiss.

(xix) Synopsys v. AzurEngine

Synopsys applied access control measures to its EDA software in the form of a license key system that required licensees to input an encrypted key code that could be obtained only from Synopsys. Through use of monitoring programs, Synopsys determined that individuals associated with the defendant, which had no current license to the Synopsys software, had impermissibly accessed its software using counterfeit license keys that tricked the company's license control systems into thinking the defendant was a licensed user.¹⁰³³

Synopsys sought a TRO against this behavior, which the court granted. The defendant argued that its use of Synopsys software was authorized because an unnamed "Chinese business partner" had purportedly provided it with valid licensed access to the Synopsys software. The court ruled that, even if it were true that the defendant had a valid license, that would not allow the company to use counterfeit keys to circumvent Synopsys's software protections. The court held that even lawful purchasers must establish that they had specific authorization to circumvent in order to avoid DMCA liability.¹⁰³⁴

The court also rejected the defendant's argument that Synopsys could not apply the DMCA extraterritorially on the ground that access to Synopsys' software occurred through the defendant's servers in China. The court noted the conduct that is the focus of Section 1201(a)(1) – gaining access to copyrighted works by circumventing technological access controls – occurred in the United States where the Synopsys software was stored, and thus application of the DMCA to the defendant's U.S.-based circumventions was a permissible domestic application of the DMCA even if other conduct occurred abroad.¹⁰³⁵

**(xx) In re Dealer Mgmt. Sys. Antitrust Litig. – Secondary Liability
Under Section 1201(a)**

This case involved antitrust litigation related to CDK Global, LLC's enterprise software and computing platform for automotive dealerships and dealership groups known as its Dealer Management System or DMS. CDK brought counterclaims against several counter-defendants alleging that they repeatedly breached their contracts with CDK by handing out their DMS login credentials, directly or through their software vendors, to third party data extractors for the express purpose of enabling those third parties to use the credentials to repeatedly access CDK's DMS using computer software that scraped large volumes of data from the system. Many of

¹⁰³³ Synopsys, Inc. v. AzurEngine Techs., Inc., 401 F. Supp. 3d 1068, 1071 (S.D. Calif. 2019).

¹⁰³⁴ Id. at 1073.

¹⁰³⁵ Id. at 1074.

those data extractors – including Authenticom – then resold that data to other third party application providers, paying nothing to CDK. CDK alleged that counter-defendants Continental and Warrensburg worked with Authenticom, in violation of Section 1201(a)(1)(A), to evade CDK’s efforts to disable the login credentials by having new credentials created or by restoring disabled credentials, and installed Authenticom’s software tool in an attempt to reenable passwords that CDK had disabled.¹⁰³⁶

Continental and Warrensburg argued that they could not be held secondarily liable under Section 1201(a)(1)(A) of the DMCA, citing cases holding that there is no secondary liability under various other statutes in the absence of the words “aid” or “abet” in the statute indicating congressional intent to establish secondary liability. The court noted that the absence of such words does not establish that imposing any kind of secondary liability under the DMCA is improper, especially in view of the relationship between the DMCA and the Copyright Act, which does impose such liability. And the court further observed that, despite the absence of language in the copyright statute expressly addressing secondary liability, courts have long imposed both vicarious and contributory liability for copyright infringement. The court also noted that several courts have applied secondary liability principles drawn from copyright law to other provisions of the DMCA, and the court could see no reason that common law secondary liability principles would apply to those provisions but not to Section 1201(a)(1).¹⁰³⁷

The counter-defendants further argued against extending secondary liability principles to Section 1201(a) because that provision created a distinct anti-circumvention right without any infringement nexus requirement. Thus, attaching a copyright context to this provision of the statute would be improper. The court disagreed, observing that the Supreme Court noted in Sony that the secondary liability principles applied in copyright law stemmed from more generally applicable common law principles. The court therefore concluded that the counter-defendants had not identified any basis for concluding that such principles should not also apply to Section 1201(a).¹⁰³⁸

¹⁰³⁶ In re Dealer Mgmt. Sys. Antitrust Litig., 2019 U.S. Dist. LEXIS 149288 at * 16, *20-21 & *50 (N.D. Ill. Sept. 3, 2019).

¹⁰³⁷ Id. at *51-52.

¹⁰³⁸ Id. at 52-53. The court went on to note that CDK had alleged facts sufficient to establish that the counter-defendants themselves circumvented a technological measure that effectively controlled access. The court observed that although it is true that the use of valid username/password combinations alone is insufficient to establish liability under Section 1201(a)(1)(A), CDK had alleged that Continental and Warrensburg did more than simply provide Authenticom with valid passwords. Specifically, CDK claimed that they took affirmative steps – including the installation of computer programs and/or the use of other automated programs – to circumvent CDK’s efforts to prevent Authenticom’s alleged unauthorized access of its DMS. For example, CDK alleged that Continental and Warrensburg worked to evade blocking by having new credentials created and/or by restoring disabled credentials. Id. at *53-54.

(2) Prohibition on Devices

In addition to proscribing acts of circumvention conduct, the DMCA also outlaws devices and technology directed to circumvention of technological copyright protection measures. Specifically, Sections 1201(a)(2) and 1201(b) prohibit the manufacture, import, offer to the public, or trafficking in any technology, product, service, device, component, or part thereof that is primarily designed or produced for the purpose of circumventing a technological measure that effectively “controls access to” a copyrighted work or “protects a right of a copyright owner,” or has only limited commercially significant purpose or use other than to circumvent such technological measure, or is marketed for use in circumventing such technological protection measure. Section 1201(b)(2) provides that a technological measure “effectively protects a right of a copyright owner” if the measure “in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner.” Although trafficking in these types of prohibited devices might well constitute contributory infringement, Sections 1201(a)(2) and 1201(b) make it a direct statutory violation subject to criminal and civil penalties.

It should be noted that, although Sections 1201(a)(2) and 1201(b) in combination prohibit devices designed to circumvent both technological measures that control access to a copyrighted work and that protect a right of a copyright owner, Section 1201(a)(1) prohibits conduct that is directed only to the former, but not the latter. The rationale for this distinction was apparently a belief that anyone should be free to circumvent a measure protecting rights of a copyright owner in order to make fair use of a work,¹⁰³⁹ whereas gaining access in the first instance to a copyrighted work without the owner’s permission cannot be a fair use.¹⁰⁴⁰

Unlike the case of the prohibition of circumvention to gain unauthorized access to a work under Section 1201(a)(1), the prohibitions of Sections 1201(a)(2) and 1201(b) were not suspended for a two year period and went into effect immediately under the DMCA. Thus, the DMCA set up the curious situation in which, for the initial two year period, it did not directly prohibit circumvention of a technological measure to gain access to a work, but did prohibit the manufacture, sale or importation of devices that would enable or assist one to gain such access.

¹⁰³⁹ See The Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary (Dec. 1998) at 4 (explaining that the distinction between Section 1201(a) and (b) as to the act of circumvention in itself was “to assure that the public will have the continued ability to make fair use of copyrighted works. Since copying may be a fair use under appropriate circumstances, *section 1201* does not prohibit the act of circumventing a technological measure that prevents copying.”). Similarly, the Copyright Office noted in its rationale for the first set of exemptions it established from the prohibition against circumvention of technological measures controlling access to a work: “The decision not to prohibit the conduct of circumventing copy controls was made, in part, because it would penalize some noninfringing conduct such as fair use.” 65 Fed. Reg. 64556, 64557 (Oct. 27, 2000).

¹⁰⁴⁰ *Realnetworks, Inc. v. DVD Copy Control Ass’n*, 641 F. Supp. 2d 913, 942 (N.D. Cal. 2009) (“The prohibition on individual circumvention conduct only applies with respect to access protection technologies (because fair use can never be an affirmative defense to the act of gaining unauthorized access), not to technologies that prevent copying.”); Inna Fayenson, “Anti-Circumvention Provisions of The Digital Millennium Copyright Act,” *Journal of Internet Law*, Apr. 1999, at 9, 10.

Another curious aspect of the DMCA is that it authorizes the Librarian to create additional exceptions via rulemaking only to Section 1201(a)(1), but not to Sections 1201(a)(2) and 1201(b). Thus, the DMCA appears to allow the Librarian to permit acts of circumvention in additional situations, but not the devices necessary to enable or assist such acts.

(i) Sony Computer Entertainment America v. Gamemasters

In this lawsuit, Sony Computer Entertainment America (SCEA) obtained a preliminary injunction against the defendants, who were distributing a device called the “Game Enhancer” that enabled players to play Sony PlayStation games sold in Japan or Europe, and intended by SCEA for use exclusively on Japanese or European PlayStation consoles, on U.S. PlayStation consoles.¹⁰⁴¹ The Sony PlayStation console was designed to operate only when encrypted data was read from a game CD-ROM verifying that the CD was an authorized, legitimate product licensed for distribution in the same geographical territory of the console’s sale.¹⁰⁴²

The Game Enhancer enabled a player to trick a U.S. PlayStation console into playing a Japanese or European authorized game CD by the following method. After inserting an authorized CD game, the user was instructed to hold down the disk cover switch of the console while keeping the lid or disk cover open. The Game Enhancer was then turned on and its internal operating system selected for execution, thereby replacing the PlayStation console’s internal operating system. The validity and territorial codes were read from the authorized CD, thereby instructing the console that the inserted CD was valid and authorized. The user was then instructed to hit the “select” button on the game controller to signal the console to stop the CD motor, enabling the player to remove the U.S. authorized game CD and replace it with a CD that was authorized for play only on a Japanese or European console. Once the game was loaded, the Game Enhancer then returned control to the PlayStation’s operating system, and the unauthorized game could be played.

The court ruled that, because the Game Enhancer was a device whose primary function was to circumvent the mechanism on the PlayStation console that ensured the console operated only when encrypted data was read from an authorized CD-ROM, the Game Enhancer had a primary function to circumvent a technological measure that effectively controls access to a copyrighted work and was therefore a violation of Section 1201(a)(2)(A). The court ruled that SCEA was therefore entitled to a preliminary injunction against sale of the device under Section 1203.¹⁰⁴³

¹⁰⁴¹ Sony Computer Entertainment America v. Gamemasters, 87 F. Supp. 2d 976, 981 (N.D. Cal. 1999).

¹⁰⁴² Id.

¹⁰⁴³ Id. at 987-88. A similar case finding a violation of the DMCA as a result of sales of a cable descrambler and decoder is CSC Holdings, Inc. v. Greenleaf Electronics, Inc., 2000 U.S. Dist. LEXIS 7675 (N.D. Ill. 2000).

(ii) The DirecTV Cases

a. DirecTV, Inc. v. Borow

This straightforward case found defendant Randy Borow in violation of Section 1201(a)(1) for using an emulator to circumvent DirecTV's encryption on its signals and to simulate certain functions of the DirecTV access card in order to watch DirecTV's programming without paying subscription fees.¹⁰⁴⁴

b. DirecTV, Inc. v. Carrillo

In this case, the court found the defendant liable under Section 1201 based on his possession and transfer of equipment used to pirate satellite TV signals. The court found that the devices were primarily designed to intercept encrypted signals.¹⁰⁴⁵

(iii) Sony Computer Entertainment America v. Divineo

In Sony Computer Entertainment America, Inc. v. Divineo,¹⁰⁴⁶ the court granted summary judgment to the plaintiff that several devices sold by the defendant violated the anti-circumvention provisions of the DMCA. The devices all could be used to circumvent an authentication process designed by Sony into the Playstation system to verify that an inserted disc was authentic before the Playstation would play it. If a user burned a copy of a copyrighted Playstation game, a unique code that was part of every authentic disc would not be copied, thus preventing the user from playing the copy on the Playstation. The defendant sold the following devices that could be used to circumvent this process: (i) HDLoader, software that permitted a user to make an unauthorized copy of Playstation-compatible video games onto a separate hard drive connected to the Playstation system; (ii) mod chips that, when wired to a Playstation console, circumvented the authentication system and allowed the system to play the unauthorized software; and (iii) devices that allowed a user to boot up a Playstation console and perform a disc swap without triggering the software and hardware mechanisms within the Playstation that initiated the authentication system.¹⁰⁴⁷

The defendant argued against liability on the ground that there were several ways in which the devices could be used that did not result in infringement of the plaintiff's copyrighted video games. First, the devices could be used to allow more than 150 items of "homemade" software to execute on the Playstation. Second, software developers could use the devices to test their own games as a less expensive alternative to purchasing a specialized Sony console that would run any game. Third, HDLoader made playing games more convenient by allowing users to avoid having to swap out discs to change games and because the Playstation could read

¹⁰⁴⁴ DirecTV, Inc. v. Borow, 2005 U.S. Dist. LEXIS 1328 at *3, *12-13 (N.D. Ill. Jan. 6, 2005).

¹⁰⁴⁵ DirecTV, Inc. v. Carrillo, 227 Fed. Appx. 588, 589-90 (9th Cir. 2007).

¹⁰⁴⁶ 457 F. Supp. 2d 957 (N.D. Cal. 2006).

¹⁰⁴⁷ Id. at 958-59.

hard drive data more quickly than data stored on CDs or DVDs. The defendant also gave a legal notice on its web site warning users that they were responsible for the legality of their own use of materials obtained through the web site.¹⁰⁴⁸ The defendant also invoked the reverse engineering defense of Section 1201(f) of the DMCA, arguing that users of mod chips could use them to ensure the interoperability of an independently created computer program with the Playstation.¹⁰⁴⁹

The court rejected all of these arguments, holding that the challenged devices were primarily designed for the purpose of circumventing the Playstation authentication system which otherwise controlled access to software played on the system, and that “downstream customers’ lawful or fair use of circumvention devices does not relieve [defendant] from liability for trafficking in such devices under the DMCA.”¹⁰⁵⁰ The court also ruled that the defendant’s legal notice to users of its devices was not relevant to its own liability under the DMCA.¹⁰⁵¹ The application of the court’s ruling to the Section 1201(f) interoperability rights is interesting. It means that, even though it may be permissible to circumvent a technological measure to obtain information necessary for interoperability of an independently developed computer program, or for the user of an independently developed computer program to circumvent an access control measure in order to interoperate with a program controlled by the measure, it is nevertheless illegal for a third party to sell such user a device that would enable the circumvention, if the device is designed primarily for circumvention. Another implication of the ruling is that legal uses that may result after use of a device to accomplish circumvention are not to be factored into whether the device is primarily designed for circumvention. Under this decision, the DMCA focuses only on the capability of the device to accomplish circumvention in the first instance, and if that is its primary technical function, it is illegal.

(iv) Ticketmaster L.L.C. v. RMG Technologies, Inc.

In this case, the plaintiff Ticketmaster alleged the defendant had violated Sections 1201(a)(2) and 1201(b)(1) by distributing an automated tool that enabled users (such as ticket brokers) to access and navigate rapidly through the Ticketmaster site and purchase large quantities of tickets. The tool enabled users to bypass Ticketmaster’s “CAPTCHA” system, a security system designed to distinguish between human users and automated programs by requiring the user to read a distorted sequence of letters and numbers on the screen and enter those letters and numbers correctly into the system in order to gain access to the ticket purchase page.¹⁰⁵²

¹⁰⁴⁸ Id. at 961.

¹⁰⁴⁹ Id. at 965.

¹⁰⁵⁰ Id.

¹⁰⁵¹ Id.

¹⁰⁵² Ticketmaster L.L.C. v. RMG Technologies, Inc., 507 F. Supp. 2d 1096, 1102, 1111-12 (C.D. Cal. 2007).

On a motion for a preliminary injunction, the court found the plaintiff likely to prevail on these claims. The court rejected the defendant's argument that CAPTCHA was not a system or a program that qualified as a technological measure under the DMCA because it was simply an image, and it was designed to regulate ticket sales, not to regulate access to a copyrighted work. The court ruled that the DMCA does not equate its use of the term "technological measure" with the defendant's terms "system" or "program," and that in any case the CAPTCHA system was a technological measure within the DMCA because most automated devices could not decipher and type the stylized random characters the system generated in order to proceed to the copyrighted ticket purchase pages.¹⁰⁵³ Thus, CAPTCHA qualified as a technological measure that restricted access to copyrighted works within the purview of Section 1201(a)(2). Similarly, it also fell within the purview of Section 1201(b)(1) because it protected rights of the copyright owner by preventing automated access to the Ticketmaster ticket purchase web pages, thereby preventing users from copying those pages. Accordingly, the court issued a preliminary injunction prohibiting the defendant from trafficking in any computer program or other automatic devices to circumvent copy protection systems in Ticketmaster's web site and from using any information gained from access to Ticketmaster's web site to create computer programs to circumvent Ticketmaster's copy protection and web site regulation systems.¹⁰⁵⁴

(v) The Tracfone Cases

In TracFone Wireless, Inc. v. Pak China Group Co., Ltd.,¹⁰⁵⁵ the defendants were engaged in bulk purchase, reflashing, and redistributing TracFone phones. The plaintiff brought claims under Section 1201 for circumvention and trafficking in circumvention technology. The defendants failed to answer and were in default. The court found the defendants guilty of the alleged violations of Section 1201 and imposed the maximum statutory damages of \$37,707,500 based on the sale of at minimum 15,083 reflashed TracFone prepaid phones.¹⁰⁵⁶

In TracFone Wireless, Inc. v. Technopark Co., Ltd.,¹⁰⁵⁷ the court found the defendants liable under Section 1201 for the unauthorized unlocking or reflashing of TracFone phones and for trafficking in certain unlocking devices known as "Octopus Boxes" in furtherance of its unlocking scheme. The court also found the defendants liable for facilitating co-conspirators who were trafficking in the service of circumventing TracFone's technological measures. The court imposed a maximum statutory damages award of \$10,000 for the four unlocking or reflashing devices manufactured by the defendants and sold by distributors that TracFone was aware of.¹⁰⁵⁸

¹⁰⁵³ Id. at 1112.

¹⁰⁵⁴ Id. at 1112, 1116.

¹⁰⁵⁵ 843 F. Supp. 2d 1284 (S.D. Fla. 2012).

¹⁰⁵⁶ Id. at 1301.

¹⁰⁵⁷ 2012 U.S. Dist. LEXIS 58449 (S.D. Fla. Apr. 9, 2012).

¹⁰⁵⁸ Id. at *4, *13-14 & *15-16.

In addition, see the numerous TracFone cases discussed in Section II.G.1(a)(1)(i).a above.

(vi) Movida Communications, Inc. v. Haifa

In this case, the court ruled that the defendant's actions of tampering with or altering pre-paid control software resident on Movida pre-paid wireless handsets, entering unauthorized PIN numbers into the phones for purposes of unlocking or re-flashing the phones, and reselling the phones for use on networks other than Movida's, violated Section 1201 of the DMCA. The court issued a permanent injunction against the defendant, prohibiting him even from purchasing any model of Movida handsets, in addition to re-flashing or unlocking any Movida handset, and accessing, altering, erasing, tampering with, deleting or otherwise disabling Movida's proprietary prepaid cellular software contained within any model of Movida handset. The order also provided that any violation would be punished in an amount of not less than \$5,000 per Movida handset.¹⁰⁵⁹

(vii) MDY Industries v. Blizzard Entertainment

In this case, the defendant distributed bot software called "Glider" that was able to play Blizzard Entertainment's multiplayer online role-playing game known as World of Warcraft (WoW) for its owner while the owner was away from his or her computer, thereby enabling the owner to advance more quickly within WoW than would otherwise be possible.¹⁰⁶⁰ Blizzard Entertainment brought claims under the DMCA, alleging that Glider evaded Blizzard technologies known as "Warden" to detect and prevent the use of bots by WoW players. Warden included two different software components. The first component, known as "scan.dll," scanned the user's computer for unauthorized programs such as Glider before the user logged onto the WoW servers to play the game, and if it detected such programs, scan.dll would deny the user access to the game servers. The second component, known as the "resident" component of Warden, ran periodically while a user played WoW and if it detected the use of a bot program, Blizzard would revoke access to the game.¹⁰⁶¹

Blizzard argued that scan.dll and the resident software controlled access to copyrighted software, as required by Section 1201(a)(2) of the DMCA, in two ways. First, when scan.dll prevented a user from playing WoW, or when the resident software terminated a user's playing of WoW, they prevented additional code in the game client software from being written to RAM. Second, scan.dll and the resident software barred access to WoW's non-literal elements (the multi-media presentation of the WoW universe and character interactions) generated by the code's interaction with the computer hardware and operating systems.¹⁰⁶²

¹⁰⁵⁹ Movida Communications, Inc. v. Haifa, 2008 Copyr. L. Dec. ¶ 29,528 (C.D. Cal. 2008).

¹⁰⁶⁰ MDY Industries, LLC v. Blizzard Entertainment, Inc., 2008 U.S. Dist. LEXIS 53988 at *2 (D. Ariz. 2008 July 14, 2008).

¹⁰⁶¹ Id. at *34.

¹⁰⁶² Id. at *34-35.

The court rejected Blizzard's claim under Section 1201(a)(2). With respect to access to the code of WoW, the court, citing the Lexmark case, ruled that a holder of Blizzard's game client software had full and complete access to that code on both the CD that contained it and on the user's hard drive once the software had been loaded onto the user's computer. The user thereafter could view a copy of the game client software code, regardless of whether the user actually played WoW or encountered Warden. The user did not need to pass through Blizzard's security devices to gain access to the code. Accordingly, the court granted summary judgment to the defendant on this issue. The court ruled that it could not similarly grant summary judgment with respect to the non-literal elements of WoW because the parties' statement of facts filed in conjunction with their motions for summary judgment said virtually nothing about this aspect of the game. Finally, the court noted that neither scan.dll nor the resident software appeared to require the application of information by the game user, or the application of a process or a treatment by the game user, before granting access to copyrighted information, as required by Section 1201(a)(2). Instead, they merely scanned for unauthorized programs. However, because neither party had addressed this issue in their briefs, the court noted that it would be a factual issue for trial.¹⁰⁶³

The court also rejected a claim by Blizzard under Section 1201(b)(1) of the DMCA. Blizzard asserted that scan.dll and the resident software prevented users from copying software code to RAM and accessing the non-literal elements of the game once they were caught using Glider. MDY disputed this factual assertion, contending that code from the game client software was not written to RAM after a user passed by scan.dll or the resident software. The court concluded that, because there was a factual dispute with respect to the extent to which Blizzard's Warden software protected against the copying of software code to RAM, and because the parties did not submit sufficient facts from which the court could decide whether the protective measures protected Blizzard's rights in the non-literal elements of the game, summary judgment on the Section 1201(b)(1) claim was denied.¹⁰⁶⁴

In a subsequent opinion issued after a bench trial, the court held that Blizzard's circumvention claims against Glider under Sections 1201(a)(2) and 1201(b)(1) failed with respect to the discrete nonliteral components of the games stored on the game player's hard drive, because they could be accessed and viewed without signing onto the server (and therefore involving the Warden software) by independently purchased computer programs that could call up the individual visual images or recorded sounds within the game client software. However, the circumvention claims were valid with respect to the "dynamic" nonliteral elements of WoW – i.e., the real-time experience of traveling through different worlds, hearing their sounds, viewing their structures, encountering their inhabitants and monsters, and encountering other players – because those dynamic elements could be accessed and copied only when the user was connected to a Blizzard server that controlled their dynamic display, which in turn required

¹⁰⁶³ Id. at *18, *35-40.

¹⁰⁶⁴ Id. at *41-43.

the user successfully to pass scan.dll when logging on and to survive the periodic scrutiny of the resident component.¹⁰⁶⁵

Six weeks later, the court entered two permanent injunctions against the marketing, sale and distribution of Glider for use in connection with WoW – one on the basis of the copyright infringement and DMCA claims, and another on the basis of a tortious interference with contract claim for which the court had ruled in favor of Blizzard. The court stayed the injunction on the copyright and DMCA claims pending their appeal, but refused to stay the injunction on the tortious interference claims.¹⁰⁶⁶ In a subsequent opinion, the court awarded Blizzard statutory damages of \$6.5 million.¹⁰⁶⁷

On appeal, the Ninth Circuit reversed, except as to MDY's liability for violation of Section 1201(a)(2).¹⁰⁶⁸ The Ninth Circuit cast one of the key issues on appeal to be whether the DMCA's anti-circumvention provisions prohibit circumvention of access controls only when unauthorized access leads to copyright liability, as the Federal Circuit had held in the Chamberlain and Storage Tech cases.¹⁰⁶⁹ The Ninth Circuit reached a conclusion contrary to the Federal Circuit on that issue.¹⁰⁷⁰

First, the Ninth Circuit noted textual differences between the prohibitions of Section 1201(a) and 1201(b). Section 1201(a) is directed to protecting a "work protected under this title," whereas Section 1201(b) is directed to protecting "a right of a copyright owner."¹⁰⁷¹ Noting that neither Section 1201(a)(1) nor 1201(a)(2) explicitly refer to traditional copyright infringement under Section 106, the court read Section 1201(a) "as extending a new form of protection, i.e., the right to prevent circumvention of access controls, broadly to works

¹⁰⁶⁵ MDY Industries, LLC v. Blizzard Entertainment, Inc., 616 F. Supp. 2d 958, 964-68 (D. Ariz. 2009). The court noted that Warden did not prevent all WoW users from copying the dynamic nonliteral elements of the game because players who did not use Glider could copy that content while connected to Blizzard servers. The court noted, however, that Section 1201(b)(1)(A) requires only that the technological measure restrict or otherwise limit *unauthorized* copying. Id. at 968 n.3.

¹⁰⁶⁶ MDY Industries, LLC v. Blizzard Entertainment, Inc., 2009 U.S. Dist. LEXIS 24151 (Mar. 10, 2009). The court denied a motion for reconsideration of the denial of the stay of the tortious interference injunction. MDY Industries, LLC v. Blizzard Entertainment, Inc., 2009 U.S. Dist. LEXIS 25650 (Mar. 25, 2009).

¹⁰⁶⁷ MDY Industries, LLC v. Blizzard Entertainment, Inc., 2009 U.S. Dist. LEXIS 38260 (D. Ariz. Apr. 1, 2009).

¹⁰⁶⁸ MDY Industries, LLC v. Blizzard Entertainment, Inc., 2011 U.S. App. LEXIS 3428 (9th Cir. Feb. 17, 2011).

¹⁰⁶⁹ Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004); Storage Technology Corp. v. Custom Hardware Eng'g Consulting, Inc., 421 F.3d 1307 (Fed. Cir. 2005).

¹⁰⁷⁰ The court also rejected MDY's contention that Warden's scan.dll and resident components were separate, and only scan.dll should be considered as a potential access control measure under Section 1201 (a)(2). The court held that "an access control measure can both (1) attempt to block initial access and (2) revoke access if a secondary check determines that access was unauthorized. Our analysis considers Warden's scan.dll and resident components together because the two components have the same purpose: to prevent players using detectable bots from continuing to access WoW software" MDY Industries, 2011 U.S. App. LEXIS at *27.

¹⁰⁷¹ Id. at *29-30.

protected under Title 17, i.e., copyrighted works.”¹⁰⁷² The court also noted that the two specific examples of unlawful circumvention recited under Section 1201(a) – descrambling a scrambled work and decrypting an encrypted work – are acts that do not necessarily infringe or facilitate infringement of a copyright. Descrambling or decrypting do not necessarily result in someone’s reproducing, distributing, publicly performing, or publicly displaying the copyrighted work, or creating derivative works based on the copyrighted work.¹⁰⁷³

In addition, the court noted another significant difference between Section 1201(a) and Section 1201(b) in that Section 1201(a)(1)(A) prohibits circumventing an effective access control measure, whereas Section 1201(b) prohibits trafficking in circumvention devices, but does not prohibit circumvention itself because, as the Senate Judiciary Committee report noted, such conduct was already outlawed as copyright infringement, so no new prohibition was necessary.¹⁰⁷⁴ Accordingly, the court concluded, “This difference reinforces our reading of § 1201(b) as strengthening copyright owners’ traditional rights against copyright infringement and of § 1201(a) as granting copyright owners a new anti-circumvention right.”¹⁰⁷⁵ The court found the legislative history of the anti-circumvention provisions of the DMCA to reinforce its reading that Section 1201(a) creates a new anti-circumvention right distinct from copyright infringement, while Section 1201(b) strengthens the traditional prohibition against copyright infringement.¹⁰⁷⁶

The Ninth Circuit noted that its reading of the anti-circumvention provisions put it in conflict with the Federal Circuit’s decisions in the Chamberlain and Storage Tech cases, in which the Federal Circuit required Section 1201(a) plaintiffs to demonstrate that the circumventing technology infringes or facilitates infringement of the plaintiff’s copyright – what the Ninth Circuit referred to as an “infringement nexus requirement.”¹⁰⁷⁷ Although the Ninth Circuit stated that it appreciated the policy considerations expressed by the Federal Circuit in Chamberlain, the Ninth Circuit found itself unable to follow the Federal Circuit’s infringement nexus requirement because it is contrary to the plain language of the statute and would lead to statutory inconsistencies in the DMCA. For example, under the Federal Circuit’s construction, Congress’s creation of a mechanism in Section 1201(a)(1)(B)-(D) for the Librarian of Congress to

¹⁰⁷² Id. at *31.

¹⁰⁷³ Id.

¹⁰⁷⁴ Id. at *32.

¹⁰⁷⁵ Id. The court also noted that, if a copyright owner puts in place an effective measure that both (1) controls access and (2) protects against copyright infringement, a defendant who traffics in a device that circumvents that measure could be liable under both Sections 1201(a) and 1201(b). Id. at *35.

¹⁰⁷⁶ Id. at *35-40.

¹⁰⁷⁷ Id. at *40.

grant exemptions to certain non-infringing behavior from Section 1201(a)(1) liability would be unnecessary if an infringement nexus requirement existed.¹⁰⁷⁸

Turning to application of its construction of the anti-circumvention provisions to the facts of the case, the Ninth Circuit agreed with the district court that Glider did not violate Section 1201(a)(2) with respect to WoW's literal elements and individual non-literal elements, because Warden did not effectively control access to those WoW elements. The literal elements (the game client's software code) were available on a player's hard drive once the game client software was installed, and the non-literal components could be accessed by a user without signing on to the server by using independently purchased computer programs to call up the visual images or the recorded sounds within the game client software stored in files on the hard disk. Because a player needed not encounter Warden to access WoW's individual non-literal elements, Warden did not effectively control access to those elements.¹⁰⁷⁹ On this point, the Ninth Circuit finds its conclusion in accord with the Sixth Circuit's decision in the Lexmark case,¹⁰⁸⁰ in which mere purchase of one of the plaintiff's printers allowed "access" to the copyrighted program, because it could be read directly from the printer memory without encountering the printer's authentication sequence.¹⁰⁸¹

The court next found Blizzard to be liable for trafficking in violation of Section 1201(a)(2) with respect to WoW's dynamic non-literal elements, which constituted a copyrighted work available only through the WoW server. The Ninth Circuit noted a split between other circuits with respect to the meaning of the phrase "circumvent a technological measure ... without the authority of the copyright owner." The Federal Circuit concluded in Chamberlain that the definition of "circumvent a technological measure" imposes an additional requirement on a Section 1201(a)(2) plaintiff: to show that the defendant's circumventing device enables third parties to access the copyrighted work without the copyright owner's authorization (citing Chamberlain, 381 F.3d at 1193).¹⁰⁸² The Second Circuit adopted a different view, "that § 1201(a)(3)(A) plainly exempts from § 1201(a) liability those whom a copyright owner authorizes to circumvent an access control measure, not those whom a copyright owner authorizes to access the work" (citing Corley, 273 F.3d at 333 & n.15).¹⁰⁸³ The Ninth Circuit found "the Second Circuit's view to be the sounder construction of the statute's language, and [we] conclude that § 1201(a)(2) does not require a plaintiff to show that the accused device enables third parties to access the work without the copyright owner's authorization. Thus, Blizzard has satisfied the

¹⁰⁷⁸ Id. at *45-46. The Ninth Circuit noted, that like the Chamberlain court, it need not reach the question of the relationship between fair use and violations of Section 1201. MDY had not claimed that Glider use was a fair use of WoW's dynamic non-literal elements. Accordingly, the court left open the question whether fair use might serve as an affirmative defense to a prima facie violation of Section 1201. Id. at *48 n.12.

¹⁰⁷⁹ Id. at *52-53.

¹⁰⁸⁰ See Section II.G.1(a)(15)(i) below.

¹⁰⁸¹ Id. at *53-54.

¹⁰⁸² Id. at *56 n.16.

¹⁰⁸³ Id.

‘circumvention’ element of a § 1201(a)(2) claim, because Blizzard has demonstrated that it did not authorize MDY to circumvent Warden.”¹⁰⁸⁴

The Ninth Circuit found, however, that MDY was not liable under Section 1201(b)(1) because Warden did not protect MDY’s reproduction right against unauthorized copying. Although WoW players copied the software code into RAM while playing the game, Blizzard’s end user license agreement and Terms of Use authorized all licensed WoW players to do so. Because the court had found that the prohibition in the Terms of Use on use of bots was a contractual covenant rather than a condition to the license,¹⁰⁸⁵ violation of the covenant by a Glider user did not make the user a copyright infringer by continuing to copy code into RAM. Second, although WoW players could theoretically record game play by taking screen shots, there was no evidence that Warden detected or prevented such allegedly infringing copying. Warden had been designed to reduce the presence of cheats and bots, not to protect WoW’s dynamic non-literal elements against copying. Accordingly, the court ruled that Warden did not effectively protect any of Blizzard’s rights under the copyright act, and MDY was therefore not liable under Section 1201(b)(1) for Glider’s circumvention of Warden.¹⁰⁸⁶

(viii) **Coupons, Inc. v. Stottlemire**

The plaintiff offered coupon printing software that enabled online, printable coupons to be delivered to consumers. The software placed a registry key file on the user’s personal computer that acted as a counter, limiting the number of times each coupon could be printed on that computer (typically, two prints per coupon). The defendant discovered how to remove the counter, created a computer program that automated its removal, and distributed the program. The plaintiff alleged that, because each coupon had its own unique bar code and date stamp, the coupons were subject to copyright protection, and the defendant’s distribution of its computer program violated the DMCA by allowing users to access more than the limit for each coupon. The plaintiff also claimed that the act of printing constituted unauthorized copying. The defendant brought a motion to dismiss.¹⁰⁸⁷ The court found fault with the plaintiff’s DMCA claims:

These concepts seem to be logically inconsistent and, when asserted together, do appear to blur the carefully constructed distinction between “access controls” and “rights controls.” If the court accepts Coupons’ argument that each coupon is “unique,” then can there be a claim of improper copying? On the other hand, if the coupons are not unique, then the allegations against Stottlemire appear to fall within the “rights controls”

¹⁰⁸⁴ Id.

¹⁰⁸⁵ See Section III.C.2(i) below.

¹⁰⁸⁶ 2011 U.S. App. LEXIS 3428 at *60-61.

¹⁰⁸⁷ Coupons, Inc. v. Stottlemire, No. CV 07-03457 HRL (N.D. Cal. July 2, 2008), slip op. at 1, 4.

(i.e., permitting users to print more copies of coupons than were authorized by Plaintiff).¹⁰⁸⁸

The court was also not convinced that the addition of a bar code or other functional device on the coupon qualified it as a unique copyrighted work. But in any event, if Coupons wanted to make the argument, then the court noted that it needed to actually allege it in the complaint, and the plaintiff's reference to "unique coupons" in the complaint was not sufficient to put the defendant on notice of the claims against him. The court ruled that the plaintiff needed to clarify which theory it was pursuing (a "unique" coupon theory or a "general" coupon theory). Accordingly, the court dismissed the DMCA cause of action with leave to amend the complaint to clarify whether the plaintiff was asserting a claim under a Section 1201(b) "rights controls" theory (i.e., allowing users to print more than the authorized number of copies) or a claim under a Section 1201(a) "access controls" theory (i.e., "unique" coupons).¹⁰⁸⁹

After the plaintiff amended its complaint, the defendant again brought a motion to dismiss, which the court denied.¹⁰⁹⁰ In the amended complaint, the plaintiff claimed that each printed coupon's identification number marked it as an authorized copy of a copyrighted work, and did not create a derivative work. The plaintiff asserted claims under both Sections 1201(a) and 1201(b). The court ruled that the plaintiff had sufficiently alleged facts that its software controlled access to the printing of the copyrighted coupon to state a claim under Section 1201(a). With respect to Section 1201(b), the court ruled that the plaintiff had adequately alleged that its software controlled copying and distribution in two ways: the registry key limited the number of coupons distributed to a single computer (simultaneously limiting the number of authentic copies that the computer could print), and the software's counter limited the number of authentic coupons distributed as a whole. The court held that, although the plaintiff would have to prove that its software actually worked as both an access and use control, it had sufficiently alleged facts that supported its theory that the defendant had violated Section 1201(b), and the motion to dismiss was denied.¹⁰⁹¹

(ix) CoxCom, Inc. v. Chafee

CoxCom leased cable boxes to its subscribers that enabled them to descramble incoming signals for viewing and that transmitted certain information from subscribers back to CoxCom, including billing information associated with purchase of pay-per-view programming. The defendant sold a digital cable filter that filtered out low-frequency signals, including the return transmissions from the cable box containing purchase information. The court noted that the filters were not illegal, and had innocuous uses, such as allowing cable television subscribers to enhance viewing quality by filtering out interference from FM radio broadcast towers, shortwave

¹⁰⁸⁸ *Id.* at 4-5.

¹⁰⁸⁹ *Id.* at 5.

¹⁰⁹⁰ *Coupons, Inc. v. Stottlemire*, 588 F. Supp. 2d 1069, 1072 (N.D. Cal. 2008).

¹⁰⁹¹ *Id.* at 1073-75.

radios, and home appliances. However, the defendants marketed the filters to their customers as capable of filtering out pay-per-view charges.¹⁰⁹² The plaintiffs brought claims under the DMCA anti-circumvention provisions and the district court granted summary judgment to the plaintiffs on those claims.¹⁰⁹³

On appeal, the First Circuit affirmed, rejecting the defendants' argument that their filters did not "circumvent" technological measures. The court found the technological measure at issue to be CoxCom's pay-per-view delivery and billing system that scrambled pay-per-view programming to make it not viewable unless subscribers chose to purchase it.¹⁰⁹⁴ Without further analysis, the First Circuit simply concluded: "A digital cable filter allows subscribers to 'avoid' or 'bypass' that technological measure. Given the factual record, we have little trouble concluding that the district court properly granted summary judgment to CoxCom as to appellants' liability under the DMCA."¹⁰⁹⁵

(x) The DISH Network Cases

a. Dish Network v. Sonicview

DISH Network transmitted encrypted programming signals that were then received by an EchoStar receiver, which processed and decrypted the signals using data and encryption technology stored in a DISH Network access card loaded into the receiver. The access card communicated with the receiver to assure that only signals the subscriber was authorized to receive would be decrypted. DISH Network brought anti-circumvention claims against the defendants, whom DISH Network alleged were involved in the manufacture of receivers, software and other devices used to intercept and steal DISH Network's encrypted signals. Upon a motion for a TRO, the court ruled that DISH Network's security access cards functioned as both access controls and copyright controls, and that the defendants' distribution of software files through a website that allowed individuals to decrypt and view DISH Network content likely violated both Section 1201(a)(2) and 1201(b)(1).¹⁰⁹⁶

b. Dish Network v. SatFTA

In Dish Network v. SatFTA,¹⁰⁹⁷ the court found the defendant liable under Section 1201(a)(2) for trafficking in circumvention devices that aided in circumvention of Dish Network's signal and content security measures in its receivers, including software that facilitated the unauthorized re-programming of Dish Network smartcards, circuit diagrams that could be used

¹⁰⁹² CoxCom, Inc. v. Chafee, 536 F.3d 101, 104-05 (1st Cir. 2008).

¹⁰⁹³ Id. at 106.

¹⁰⁹⁴ Id. at 110.

¹⁰⁹⁵ Id.

¹⁰⁹⁶ Dish Network L.L.C. v. Sonicview USA, Inc., 2009 U.S. Dist. LEXIS 63429 at *2-3, *7-8 (S.D. Cal. July 23, 2009).

¹⁰⁹⁷ 2011 U.S. Dist. LEXIS 25038 (N.D. Cal. Mar. 9, 2011).

to build a connector to interface with the EEPROM in a Dish Network receiver to erase the data created by Dish Network's electronic countermeasures and continue receiving unauthorized programming, and diagrams depicting the storage locations of data that secured communication between receivers and smartcards.¹⁰⁹⁸ The court also found the defendant liable under Section 1201(b)(1) for trafficking in a program that allowed users to copy the programming of a Dish Network satellite receiver to a computer hard drive. Dish Network protected against unauthorized copying and distribution of recorded programming by saving the copyrighted content in an unrecognizable format, and the court found that to be a sufficient technological measure to invoke the protection of Section 1201(b)(1). The defendant contended that his program served a legitimate function by allowing individuals to create backup copies of their Dish Network recordings. The court rejected this defense, citing the case of Realnetworks, Inc. v. DVD Copy Control Ass'n¹⁰⁹⁹ for the rule that, although the DMCA provides for a limited fair use exception for certain end users of copyrighted works, the exception does not apply to manufacturers or traffickers. Because the defendant's program allowed a computer to overcome Dish Network's copy-control measures, it violated Section 1201(b)(1).¹¹⁰⁰

c. Dish Network v. Dimarco

The case of Dish Network LLC v. Dimarco¹¹⁰¹ involved the impoundment of technology that could be used to gain unauthorized access to Dish Network signals. When an authorized EchoStar receiver received a Dish Network signal, it forwarded part of the signal called the "entitlement control message" to a NagraStar smart card in the receiver. If the subscriber was tuned to a channel he was authorized to receive, the smart card retrieved a decryption key from its read-only memory and used the key to unlock the "control word" from the entitlement control message. The smart card then transmitted the control word back to the receiver, and the receiver used it to decode the incoming signal so the subscriber could watch the programming. Content providers like Dish Network routinely changed their decryption keys to help thwart piracy. A new form of piracy was developed called "Internet key sharing" or "IKS" whereby a pirate kept his unauthorized receiver connected to the Internet for automatic re-flashing with the newest keys, which were retrieved from an IKS server connected to multiple legitimate NagraStar smart cards. Control words obtained from the authorized smart cards were sent from the IKS server over the Internet to unauthorized receivers.¹¹⁰²

The defendants sold unauthorized receivers with decryption software and hardware, cables to connect the unauthorized receivers to the Internet for use with an IKS server, and

¹⁰⁹⁸ Id. at *3-6, *12-13. The court also found the defendant liable for personal violations of Section 1201(a)(1) for his admitted modification of Dish Network smartcards. The court rejected the defendant's defense that he had modified the smartcards only for the purpose of testing the operation of various receivers, not to receive an unauthorized satellite signal. Id. at *10-11.

¹⁰⁹⁹ 641 F. Supp. 2d 913 (N.D. Cal. 2009).

¹¹⁰⁰ Dish Network, 2011 U.S. Dist. LEXIS 25038 at *13-14.

¹¹⁰¹ 2012 U.S. Dist. LEXIS 33889 (D. Nev. Mar. 14, 2012).

¹¹⁰² Id. at *3-4.

passwords to access the IKS server which were euphemistically referred to as “extended warranty codes.” The defendants admitted that the receivers they sold were capable of being used for piracy, but argued that because they did not themselves traffic in illegal encryption keys, their products amounted to “modern day rabbit ears” for their customers to receive free satellite programming. The receivers had no built-in means of connecting to the Internet, but the defendants sold an adapter called a “WizHub” that enabled connection to the Internet.¹¹⁰³

The defendants argued that the court should not impound its WizHubs or extended warranty codes because the WizHub was simply an adapter and one could not engage in piracy without the piracy software and IKS servers. The court rejected this argument, noting that a device such as the WizHub permitting the connection of an otherwise legitimate receiver to the Internet along with a password permitting access to a server with illegally trafficked decryption keys could be said to constitute a product designed to circumvent a technological measure that effectively controlled access to a protected work. The court could not see any possible need for a person using a free-to-air satellite receiver in a legitimate way to connect that receiver to the Internet and enter a password to connect to a server whose sole purpose was the trafficking of decryption keys. The court therefore ordered the impoundment of the WizHub connectors and the extended warranty codes under Section 1203(b)(2), although not of the receivers themselves (for which the plaintiffs had not sought impoundment). The court refused, however, to seize the defendants’ web sites, which appeared to be used for the legitimate sale of free-to-air receivers.¹¹⁰⁴

d. Dish Network v. Sonicview

This case, a follow-on decision of the case described in subsection a. above, involved the same kind of “Internet Key Sharing” (or “IKS”) piracy of Dish Network signals described in the Dimarco case in the previous subsection. To enable IKS piracy, the defendants sold their Sonicview receivers, each model of which contained firmware having more than one exact match of the proprietary code and data that resided on the plaintiffs’ smart card, a particular algorithm important for encrypting and decrypting Dish Network satellite signals, and a graphical user interface. There were also strong similarities between the Sonicview receivers’ firmware and that of existing piracy firmware. The defendants also sold a serial Ethernet adapter called the iHub, which came with a 16-digit code that enabled the Sonicview receiver to access the IKS server through a dongle and an add-on module that worked in conjunction with the receiver, when loaded with piracy software, to receive Dish Network’s high-definition programming. Sonicview also operated a web site that contained piracy software available for download which was intended for use with Sonicview receivers to decrypt Dish Network’s satellite television programming.¹¹⁰⁵

¹¹⁰³ Id. at *4, *11-12.

¹¹⁰⁴ Id. at *12-15, *17.

¹¹⁰⁵ Dish Network, LLC v. Sonicview USA, Inc., 2012 U.S. Dist. LEXIS 75663 at *10-11, *13 (S.D. Cal. May 31, 2012).

The court found the defendants in violation of Section 1201(a)(2) by trafficking in the receivers, iHubs, add-on modules, and piracy software. The combination of a Sonicview receiver, iHub, and add-on module, when loaded with the piracy software, permitted unauthorized access to Dish Network's satellite programming. The court, citing two other district court decisions to the same effect, noted that potential lawful or fair use is not a defense to Section 1201(a) when its requirements are established. The court awarded statutory damages of \$200 per violation for 324,901 violations (at least 307,401 receivers and 17,500 iHubs sold), for a total award of \$64,980,200.¹¹⁰⁶

e. Dish Network v. Alejandri

In Dish Network v. Alejandri,¹¹⁰⁷ the court granted summary judgment to the plaintiffs that the defendants' sale of free-to-air receivers together with referral to service providers who could program them using the IKS piracy technology to receive Dish Network signals without payment of subscriber fees violated Section 1201(a)(1)(A) of the DMCA. The court noted that the defendants' equipment used for unlawful circumvention, which had been impounded, would be disposed of by the U.S. Marshals' Service upon order of the court at the conclusion of the proceedings.¹¹⁰⁸ The court also found a violation of Section 605(a) of the Communication Act (47 U.S.C. § 605(a)) and awarded statutory damages under that Act. The court did not award statutory damages under the DMCA – although the court's opinion does not make clear, it appears that the plaintiffs did not seek statutory damages under the DMCA.¹¹⁰⁹

f. Dish Network v. World Cable

(The facts and rulings of this case are discussed in Section II.G.1(a)(1)(vii) above.)

g. Dish Network v. Barnaby

In this case, the court granted a default judgment against the defendant for violation of Section 1201(a)(2) of the DMCA by purchasing at least 220 passcodes to the NFusion Private Server (NFPS), a subscription-based IKS service, which passcodes the defendant resold with the intent that they be used in the unauthorized decryption of the plaintiffs' satellite signals. The court awarded statutory damages of \$1,000 per passcode, for a total of \$220,000 in damages. The court permanently enjoined the defendant from, among other things, trafficking in IKS passcodes or other technology used in circumventing Dish Network's security system.¹¹¹⁰

¹¹⁰⁶ Id. at *22, *24-25 & *40-41.

¹¹⁰⁷ 2012 U.S. Dist. LEXIS 106839 (D. Puerto Rico July 30, 2012).

¹¹⁰⁸ Id. at *10-14, *21-25 & *28-29.

¹¹⁰⁹ Id. at *16-21, *25-28.

¹¹¹⁰ Dish Network v. Barnaby, 2016 U.S. Dist. LEXIS 154563 at *2-3, *9-11 & *17-18 (E.D. Tenn. Nov. 8, 2016).

(xi) Realnetworks v. DVD Copy Control Association

In Realnetworks, Inc. v. DVD Copy Control Association, Inc.,¹¹¹¹ the DVD Copy Control Association (DVDCCA) brought claims alleging that distribution of Realnetworks' RealDVD product violated the anti-trafficking provisions of the DMCA. DVDCCA licenses the Content Control System (CSS) technology, which combines multiple layers of encryption with an authentication process to protect the content on DVDs. CSS requires that a DVD drive lock upon insertion of a CSS-protected DVD and prevent access to its contents until a CSS-authorized player engages in an authentication procedure, akin to a secret handshake, to establish mutual trust. It also requires that players authenticate themselves to DVD drives to establish mutual trust, both to unlock the DVD and gain access to its protected video contents and also separately to gain access to keys stored in secure areas of the DVD, which then decrypt and descramble the DVD content. The process of authentication with the DVD drive, and subsequent content decryption, will fail if a DVD is not in the DVD drive. Finally, the CSS technology creates a system whereby content on a DVD may be played back only in decrypted and unscrambled form from the physical DVD and not any other source, such as a computer hard drive.¹¹¹²

The RealDVD product provided a variety of functions, including playing back DVDs placed in a computer's DVD drive, looking up information about the DVD from Internet databases, providing links to various information web sites relevant to the chosen DVD, and – the function at issue in the lawsuit – saving an image of the copy-protected content on the device's hard drive for later playback without the physical DVD being present.¹¹¹³

The court ruled that the CSS technology was both an access control and a copy control (the authentication process functioned as an access control and the encryption functioned as a copy control),¹¹¹⁴ and that distribution of RealDVD therefore violated the anti-trafficking provisions of both Sections 1201(a)(2) and 1201(b). RealDVD circumvented the access controls of CSS in violation of Section 1201(a)(2) by allowing access of CSS content on the hard drive without going through most of the CSS protection steps, such as DVD drive-locking, CSS authentication, and CSS bus encryption. Once RealDVD had copied a DVD, it did not authenticate the DVD drive or receive encrypted keys for playback from the hard drive. Accordingly, the process of authentication with the DVD drive, and subsequent content decryption, were thereby circumvented by RealDVD.¹¹¹⁵ RealDVD circumvented the copy

¹¹¹¹ 641 F. Supp. 2d 913 (N.D. Cal. 2009).

¹¹¹² Id. at 919-20.

¹¹¹³ Id. at 924. The RealDVD user license agreement provided, "You may use the saving functionality of the Software only with DVDs that you own. You may not use the Software to save DVDs that you do not own, such as rental or borrowed DVDs." Id. at 926.

¹¹¹⁴ Id. at 935.

¹¹¹⁵ Id. at 933.

controls of CSS in violation of Section 1201(b) by using the CSS authentication codes and algorithms to make an unauthorized copy of the DVD content.¹¹¹⁶

The court rejected a number of defenses asserted by Realnetworks. First, Realnetworks argued that CSS was not an “effective” technological measure because it had been widely cracked. The court found this fact of no moment, because the DMCA is predicated on the authority of the copyright owner, not whether or not the technological measure is a strong means of protection. The court held that it is sufficient under the statutory language if an access control prevents the easy creation *at the consumer level* of widely available and usable copies of copyrighted works.¹¹¹⁷

The court rejected Realnetworks’ argument that the copyright holder plaintiffs (the movie studios) could not bring a DMCA claim against a co-licensee to CSS technology. Realnetworks cited cases holding that copyright licenses are governed by contract law and copyright owners who enter into such licenses waive their rights to sue the licensee for copyright infringement and are limited to breach of contract claims. The court distinguished those cases, noting that the studios were not bringing copyright infringement claims, nor were they the direct licensors of CSS technology. Because Realnetworks had acted outside the scope of its license with the DVDCCA, the studios were permitted to bring circumvention claims under the DMCA.¹¹¹⁸

The court also rejected Realnetworks defenses that distribution of RealDVD was protected by the Sony doctrine because it was capable of substantial noninfringing uses and by virtue of the fact that the copying it permitted fell within the fair use rights of users who made copies for personal, noncommercial use. First, the court held that the DMCA supersedes Sony to the extent that the DMCA broadened copyright owners’ rights beyond the Sony holding. Second, the court ruled that whether consumer copying of a DVD for personal use is a fair use was not at issue, because while the DMCA provides for a limited fair use exception for certain end users of copyrighted works, the exception does not apply to manufacturers or traffickers of the devices prohibited by Section 1201(a)(2).¹¹¹⁹ “So while it may well be fair use for an individual consumer to store a backup copy of a personally-owned DVD on that individual’s computer, a federal law has nonetheless made it illegal to manufacture or traffic in a device or tool that permits a consumer to make such copies.”¹¹²⁰

¹¹¹⁶ Id. at 935.

¹¹¹⁷ Id. at 932.

¹¹¹⁸ Id. at 933.

¹¹¹⁹ Id. at 941-43.

¹¹²⁰ Id. at 942.

Accordingly, the court granted a preliminary injunction against the distribution of RealDVD.¹¹²¹

(xii) Apple v. Psystar

In Apple, Inc. v. Psystar Corp.¹¹²² Apple contended that Psystar's distribution of modified copies of its Mac OS X operating system on non-Apple computers constituted copyright infringement and illegal trafficking in circumvention devices. Apple distributed Mac OS X subject to a license agreement that prohibited its use on any non-Apple-labeled computer. Apple used lock-and-key technological measures to prevent Mac OS X from operating on non-Apple computers. Specifically, it encrypted the files of Mac OS X and used a kernel extension that communicated with other kernel extensions to locate a decryption key in the hardware and use that key to decrypt the encrypted files of Mac OS X. Psystar distributed a line of computers called Open Computers that contained copies of Mac OS X, modified to run on Psystar's own hardware, which was not authorized by Apple.¹¹²³

Psystar's had engaged in the following conduct at issue. It bought a copy of Mac OS X and installed it on an Apple Mac Mini computer. It then copied Mac OS X from the Mac Mini onto a non-Apple computer for use as an "imaging station." Once on the imaging station, Mac OS X was modified. Psystar then replaced the Mac OS X bootloader (a program that runs when a computer first powers up and locates and loads portions of the operating system into random access memory) and disabled and/or removed Mac OS X kernel extension files and replaced them with its own kernel extension files. Psystar's modifications enabled Mac OS X to run on non-Apple computers. The modified copy of Mac OS X became a master copy that was used for mass reproduction and installation onto Psystar's Open Computers.¹¹²⁴

The court first ruled that Psystar had violated Apple's exclusive right to copy Mac OS X by making copies of the modified version of OS X and installing them on non-Apple computers, and by making copies of such software in random access memory when turning on its computers running Mac OS X. The court refused to allow Psystar to assert a defense to such copying under Section 117 of the copyright statute, ruling that Psystar had waived such a defense by failing to plead it.¹¹²⁵ The court also held that distribution of Psystar's computers infringed Apple's exclusive distribution rights with respect to Mac OS X. The court rejected Psystar's defense under the first sale doctrine, based on the fact that it allegedly included a legitimately purchased Mac OS X DVD with every Psystar computer. The court held that the first sale defense under Section 109 provides immunity only when copies are lawfully made, and the master copy of the

¹¹²¹ Id. at 952.

¹¹²² 673 F. Supp. 2d 931 (N.D. Cal. 2009), aff'd, 658 F.3d 1150 (9th Cir. 2011), cert. denied, 132 S. Ct. 2374 (2012).

¹¹²³ Id. at 933-34.

¹¹²⁴ Id. at 934.

¹¹²⁵ Id. at 935. Without giving any reasons why, the court also observed that "the assertion of *Section 117* is so frivolous in the true context of how Psystar has used Mac OS X that a belated attempt to amend the pleadings would not be excused." Id. at 936.

modified Mac OS X residing on Psystar's imaging station was unauthorized, as were all the many unauthorized copies that were made from such master copy.¹¹²⁶ The court also concluded that Psystar had violated Apple's exclusive right to create derivative works by replacing the Mac OS X bootloader with a different bootloader to enable an unauthorized copy of Mac OS X to run on Psystar's computers, by disabling and removing Apple kernel extension files, and by adding non-Apple kernel extension files. The court rejected Psystar's contention that these modifications did not amount to creation of a derivative work because Apple's source code, object code and kernel extensions had not been modified. The court held that the replacement of entire files within the software while copying other portions resulted in a substantial variation from the underlying copyrighted work and therefore an infringing derivative work.¹¹²⁷

Turning to Apple's trafficking claim, the court noted that Apple's encryption of the Mac OS X operating system files, although aimed primarily at controlling access, also effectively protected its right to copy, at least for copies made in RAM. Accordingly, the encryption scheme constituted both an access control measure and a copy control measure. Psystar's distribution of "decryption software" (apparently referring to Psystar's substituted kernel extension files that obtained Apple's decryption key from the hardware and then used that key to decrypt the Mac OS X modules) violated both Section 1201(a)(1)(A) and Section 1201(b)(1) because it enabled obtaining unauthorized access to Mac OS X and resulted in an unauthorized copy of Mac OS X being loaded into RAM.¹¹²⁸

The court rejected Psystar's argument that Apple's technological protection measure was not effective because the decryption key for circumvention was publicly available on the Internet. "The fact that circumvention devices may be widely available does not mean that a technological measure is not, as the DMCA provides, effectively protecting the rights of copyright owners in the ordinary course of its operations."¹¹²⁹ Accordingly, the court granted Apple's motion for summary judgment.¹¹³⁰

The court also rejected Psystar's argument that Apple's alleged attempt to use copyright to tie Mac OS X to Apple hardware constituted copyright misuse. Because Apple had not prohibited others from independently developing and using their own operating system, it had not violated the public policy underlying copyright law or engaged in copyright misuse. The court noted that Apple had not prohibited purchasers of Mac OS X from using competitor's products. Rather, it had simply prohibited purchasers from using OS X on competitor's products.

¹¹²⁶ Id. at 937.

¹¹²⁷ Id. at 938.

¹¹²⁸ Id. at 941.

¹¹²⁹ Id. at 942 (quoting Sony Computer Entm't Am., Inc. v. Divineo, Inc., 457 F. Supp. 2d 957, 965 (N.D. Cal. 2006)).

¹¹³⁰ Psystar, 673 F. Supp. 2d at 942.

Thus, Apple's license agreement was simply an attempt to control the use of its own software.¹¹³¹

On appeal, the defendant did not challenge the district court's rulings of infringement, but rather challenged the district court's rejection of Psystar's misuse defense. The Ninth Circuit affirmed the district court's copyright misuse rulings.¹¹³² After a review of relevant misuse decisions by courts in the Ninth Circuit, the court concluded, "A software licensing agreement may reasonably restrict use of the software as long as it does not prevent the development of competing products."¹¹³³ The court found that Apple's license agreement did not impermissibly do so: "Apple's [license agreement] does not restrict competitor's ability to develop their own software, nor does it preclude customers from using non-Apple components with Apple computers. Instead, Apple's [license agreement] merely restricts the use of Apple's own software to its own hardware. ... Psystar produces its own computer hardware and it is free to develop its own computer software."¹¹³⁴ The court also rejected Psystar's reliance on the first sale doctrine, arguing that Apple was attempting to control the use of the Mac OS X software after it had been sold, because Psystar purchased retail-packaged copies of the OS. The court found that the argument falsely assumed that Apple transferred ownership of the Mac OS X when it sold a retail-packaged DVD containing software designed to enable Apple's existing customers to upgrade to the latest version of the OS. The court found that, although buyers of the DVD purchased the disc, they knew they were not buying the software, as Apple's license agreement clearly explained as much. Accordingly, the DVD purchasers were licensees, not owners, of the copies of the software.¹¹³⁵ The Ninth Circuit therefore affirmed the district court's grant of summary judgment in favor of Apple and its entry of a permanent injunction against Psystar's infringement of the Mac OS X.¹¹³⁶

(xiii) **Blizzard Entertainment v. Reeves**

In this case, the defendant ran a website that enabled its users to bypass the checks and restrictions for access to the plaintiff's World of Warcraft online gaming environment. After granting a default judgment, the court turned to what the appropriate award of statutory damages should be. The court estimated the number of circumvention violations by looking to the total number of community members on the defendant's website (427,393), each of whom was assumed to have downloaded, access or otherwise used anti-circumvention software,

¹¹³¹ Id. at 939-40.

¹¹³² Apple, Inc. v. Psystar Corp., 658 F.3d 1150, 1152 (9th Cir. 2011), cert. denied, 132 S. Ct. 2374 (2012).

¹¹³³ Id. at 1159.

¹¹³⁴ Id. at 1160.

¹¹³⁵ Id. at 1159-60.

¹¹³⁶ Id. at 1162.

services, or products offered by the defendant. The court then awarded the \$200 minimum amount per violation, for a total award of $\$200 \times 427,393 = \$85,478,600$.¹¹³⁷

(xiv) The Craigslist Cases

a. Craigslist v. Naturemarket

In Craigslist, Inc. v. Naturemarket,¹¹³⁸ the defendants distributed software that bypassed the CAPTCHA system of the Craigslist site and enabled users to post ads automatically in whatever quantity, frequency, and location the user wished, in violation of the Craigslist site Terms of Use.¹¹³⁹ Upon a motion for a default judgment, a magistrate judge issued an opinion recommending that the defendants' distribution of the software be found in violation of Sections 1201(a)(2) and 1201(b)(1) because the software "enabled unauthorized access to and copies of copyright-protected portions of Plaintiff's website controlled by [the CAPTCHA system] – particularly the ad posting and account creation portions of the website."¹¹⁴⁰ The magistrate judge also recommended an award of statutory damages in the amount of \$1,000 per copy of software distributed, estimated at 470 copies (obtained by dividing the defendants' estimated revenue of \$40,000 by the list price of \$84.95 for the software), for a total statutory damages award of \$470,000.¹¹⁴¹ The district court adopted the magistrate judge's recommendations and opinion in every respect, and entered a permanent injunction against the defendants enjoining them from distributing software that enabled postings on Craigslist without each posting being entered manually or that used automated means to download or otherwise obtain data from Craigslist, from circumventing the CAPTCHA system or other technological measures controlling access to the site, from repeatedly posting the same or similar content on the site or in more than one category, and from accessing or using the site for any commercial purpose whatsoever.¹¹⁴²

b. Craigslist v. Mesiab

In Craigslist, Inc. v. Mesiab,¹¹⁴³ a magistrate judge recommended that the plaintiff's motion for default judgment and award of statutory damages be granted based on violations of the DMCA anti-circumvention provisions in the following ways:

¹¹³⁷ Blizzard Entertainment, Inc. v. Reeves, 2010 U.S. Dist. LEXIS 85560 at *7-8 (C.D. Cal. Aug. 10, 2010).

¹¹³⁸ 694 F. Supp. 2d 1039 (N.D. Cal. 2010) (report and recommendation of magistrate judge re plaintiff's motion for default judgment).

¹¹³⁹ Id. at 1048-49.

¹¹⁴⁰ Id. at 1056.

¹¹⁴¹ Id. at 1063-64. The magistrate judge also recommended that an award of actual damages be made against the defendants based on the liquidated damages clause of the Terms of Use, which provided for \$200 for every ad the defendants posted as posting agents on behalf of users, for a total of \$840,000. Id. at 1064.

¹¹⁴² Craigslist, Inc. v. Naturemarket, Inc., 694 F. Supp. 2d 1039 (N.D. Cal. 2010) at 1046-47.

¹¹⁴³ 2010 U.S. Dist. LEXIS 134411 (N.D. Cal. Nov. 15, 2010).

– Distribution of “EasyAd Suite” software that bypassed the CAPTCHA system of the Craigslist site and enabled users to post ads automatically and in unlimited quantity. The magistrate recommended that an award of \$800 per copy sold be increased to \$1,500 per copy because the defendants had shown disregard for the injunction entered by the court. Based on 2,983 copies of the software distributed, the magistrate recommended an award of \$4,474,500.¹¹⁴⁴

– Sale or offer for sale of “CAPTCHA credits,” which was a service to circumvent CAPTCHAs through instantaneous outsourcing for occasions when the EasyAd Suite program was unable to decode the CAPTCHA. The defendants also offered CAPTCHA circumventions in bulk for prices ranging from \$12.50 for 500 credits to \$157.50 for 10,000 credits. The magistrate ruled that damages under the DMCA could properly be calculated based on offers to sell and not actual sales of CAPTCHA credits, as well as credits sold through a third party. Because it was uncontested that defendants’ web site offered to sell CAPTCHA credits and those offers were made to at least the number of people who purchased the EasyAd Poster Deluxe software, the magistrate found the defendants liable for damages for 2,983 offers. The magistrate recommended an award of \$400 per violation for offers to sell CAPTCHA credits, for an award of \$1,193,200.¹¹⁴⁵

– Offers of Craigslist telephone-verified accounts. The “Adult” and “Therapeutic Services” categories on Craigslist required telephone verification in order to post ads and the telephone-verified accounts offered by the defendants allowed purchasers to pay to have their accounts fraudulently verified by contracted employees or devices. Again applying the rule that offers for sale were sufficient for damages, the magistrate found that at least 1,000 offers for telephone-verified accounts were made, and that an award of \$400 per offer was reasonable (\$400,000 in total).¹¹⁴⁶

The district court adopted the magistrate’s recommendation in full and entered judgment against the defendants for a total statutory damages award of \$6,067,700.¹¹⁴⁷

c. Craigslist v. Hubert

In Craigslist, Inc. v. Hubert,¹¹⁴⁸ the court ruled, on an entry of default judgment after the defendant failed to appear, that the sale of software allowing users to automatically post ads to Craigslist and the provision of a service that automated and circumvented the entry of CAPTCHA passwords violated the ant-circumvention provisions of the DMCA. The court awarded statutory damages of \$400 for each of the 3,000 users of the defendant’s web site, on the theory that

¹¹⁴⁴ Id. at *30-32.

¹¹⁴⁵ Id. at *6, *33-35.

¹¹⁴⁶ Id. at *35-37.

¹¹⁴⁷ Craigslist, Inc. v. Mesiaab, 2010 U.S. Dist. LEXIS 134381 (N.D. Cal. Dec. 20, 2010).

¹¹⁴⁸ 2010 U.S. Dist. LEXIS 143037 (N.D. Cal. Apr. 15, 2010).

each user received an “offer” to circumvent in the form of an offer to purchase the defendant’s software or CAPTCHA credits, for a total award of \$1,200,000. The court rejected the plaintiff’s request for the statutory maximum of \$2,500 per offer, finding that such an award would be vastly disproportional to the actual costs the plaintiff alleged it had incurred as a result of auto-posting, \$5,000 per year.¹¹⁴⁹

d. Craigslist v. Branley

In this case, the court denied Craigslist’s request for a default permanent injunction against a defendant who failed to appear because Craigslist had not alleged facts sufficient to support the allegation that the defendant would continue to act as an agent posting ads for third parties by circumventing Craigslist’s CAPTCHA system using software known as “CLAD Genius,” in violation of Section 1201 and Craigslist’s Terms of Use.¹¹⁵⁰

e. Craigslist v. Kerbel

In this case, the court granted the plaintiff’s motion for a default judgment, finding that the plaintiff had adequately pled claims for violation of the anti-circumvention provisions based on the defendants’ alleged bypassing of Craigslist’s CAPTCHA software and its phone verification measures in order to automatically create accounts and post ads to Craigslist. The court awarded statutory damages of \$200,000, calculated on the defendants’ offer to sell a bundle of 10,000 “credits” used to purchase phone-verified accounts on Craigslist at 10 credits each, representing 1,000 offers to sell the accounts, multiplied by the minimum statutory damages award of \$200 per violation.¹¹⁵¹

(xv) Echostar v. Viewtech

In Echostar Satellite LLC v. Viewtech, Inc.,¹¹⁵² the court granted the plaintiff summary judgment on its claim under Section 1201(a)(2) against the defendants for the distribution of receivers structurally altered so as to be capable of unauthorized decryption of Echostar satellite TV programming and of software that would enable the piracy of Echostar’s programming. The court also found that the defendants’ provision of free receiver to moderators on popular piracy web sites and encouragement of the moderators to provide favorable reviews of the receiver’s ability to obtain the plaintiff’s protected programming violated the third prong of Section 1201(a)(2), which prohibits marketing a technology used in circumventing an access measure. The court awarded statutory damages of \$214,898,600, representing \$200 for each of at least 1,074,493 receivers intended for piracy sold by the defendants.¹¹⁵³

¹¹⁴⁹ Id. at *4, *10-13.

¹¹⁵⁰ Craigslist, Inc. v. Branley, 2012 U.S. Dist. LEXIS 36731 at *4-5, *12 (N.D. Cal. Mar. 19, 2012).

¹¹⁵¹ Craigslist, Inc. v. Kerbel, 2012 U.S. Dist. LEXIS 108573 at *26-27, *49-50 (N.D. Cal. Aug. 2, 2012).

¹¹⁵² 2011 U.S. Dist. LEXIS 42709 (S.D. Cal. Apr. 20, 2011).

¹¹⁵³ Id. at *4-5, *8-11.

(xvi) Adobe Systems v. Feather

In this case, the defendant offered for sale and distributed pirated copies of the plaintiffs' software via the Internet, including on eBay and through his own website. He also trafficked in and sold product keys or serial numbers designed to circumvent the plaintiffs' copyright protection measures to enable the pirated copies to function. Upon a motion for default judgment, the court found that the defendant's actions, as alleged in the complaint, established violations of Section 1201(a)(2) and of willful copyright infringement. The court awarded statutory damages for willful infringement under Section 504(c)(2) in the amount of \$90,000 for each of 28 copyrighted works infringed, for a total award of \$2,520,000 in damages. The plaintiffs did not seek separate damages for their DMCA claim, and the court noted in a footnote that they could not do so in any event, citing other authority for the proposition that a plaintiff cannot seek duplicative statutory damages under the Copyright Act and the DMCA.¹¹⁵⁴ Note that the ruling with respect to "duplicative" statutory damages seems contrary to other cases, such as the Pacific Stock v. MacArthur & Co. case discussed in Section G.1(c)(1)(xi) below, which awarded statutory damages for CMI violations in addition to statutory damages for copyright infringement arising out of the same acts.

(xvii) NNG v. AVA Enterprises

The facts and the court's rulings with respect the plaintiff's trafficking claims in this case are discussed in Section II.G.1(a)(1)(xi) above.

(xviii) Beco Dairy Automation v. Global Tech Systems

Global Tech Systems (GTS) was the owner of copyrights in software for the dairy industry. In a counterclaim in this lawsuit, GTS alleged that Beco provided third parties with tools to circumvent encryption technology that protected its software in violation of Section 1201. Beco moved to dismiss the DMCA claims or for a more definite statement of the claims. Beco argued that GTS's claims were not viable because GTS did not identify how Beco's activities affected GTS's copyrights, citing support from Federal Circuit case law.¹¹⁵⁵ The court rejected this, noting that under the Ninth Circuit's decision in MDY Industries,¹¹⁵⁶ Section 1201(a) creates a new anti-circumvention right distinct from copyright infringement. Accordingly, Section 1201(a) claims do not require a plaintiff to show that the circumvention is tied to activities that actually infringe on a copyright holder's protected rights. Moreover, GTS had alleged that Beco's circumvention

¹¹⁵⁴ Adobe Sys v. Feather, 895 F. Supp. 2d 297, 301-02 & 303 n.5 (D. Conn. 2012).

¹¹⁵⁵ Beco Dairy Automation, Inc. v. Global Tech Sys., Inc., 2015 U.S. Dist. LEXIS 130503 at *2-3, *26 (E.D. Cal. Sept. 28, 2015).

¹¹⁵⁶ MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928 (9th Cir. 2010), opinion amended and superseded on denial of reh'g, 2011 U.S. App. LEXIS 3427 (9th Cir. Feb. 17, 2011).

infringed on its copyrights when Beco engineered pirated software keys to GTS's technology and sold those keys to third parties. The court therefore denied Beco's motions.¹¹⁵⁷

(3) What Constitutes an Effective Technological Measure

(i) Auto Inspection Services v. Flint Auto Auction

In Auto Inspection Services v. Flint Auto Auction,¹¹⁵⁸ the plaintiff was the owner of an automotive inspection program that provided a uniform method of inspecting vehicles after the term of a lease or use had expired. The plaintiff included a quality control feature as part of the program that allowed it to monitor all information collected using the program. For example, when a vehicle inspector collected data for a vehicle and entered it into the program, the data had to be sent to the plaintiff for quality control inspection before the information could be forwarded to the owner of the vehicle. In this way, the plaintiff could monitor who was using the program to protect against unauthorized use.¹¹⁵⁹

The defendant, a former licensee of the plaintiff's program, wrote its own automotive inspection program to replace the plaintiff's program. The plaintiff claimed that the defendant's program was a copyright infringement. The plaintiff also claimed that its quality control feature constituted a technical protection measure to restrict access and use of its software, and that the defendant had violated the anti-circumvention provisions of the DMCA by circumventing the quality control feature to gain access to the plaintiff's source code to copy it.¹¹⁶⁰

The court found it questionable that the quality control feature was a technical measure that effectively controlled access to a protected work within the purview of the DMCA. The court noted that the protected work at issue was the source code of the program, and the user detection feature was a part of the program itself that in no way controlled access to the source code. Rather, it merely alerted the plaintiff as to who was using the program. Consequently, the user detection feature would not prevent anyone from gaining access to the source code and copying it verbatim. Moreover, the feature came into play only after a user had conducted an inspection, and did not prevent unauthorized users from accessing the program in the first instance.¹¹⁶¹

¹¹⁵⁷ Beco, 2015 U.S. Dist. LEXIS at *25-27.

¹¹⁵⁸ 2006 U.S. Dist. LEXIS 87366 (E.D. Mich. Dec. 4, 2006).

¹¹⁵⁹ Id. at *1-2.

¹¹⁶⁰ Id. at *4-5, *22.

¹¹⁶¹ Id. at *23.

(ii) Healthcare Advocates, Inc. v. Harding, Earley, Follmer &

Frailey

In Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey,¹¹⁶² the court addressed the issue of whether a robots.txt file applied to a web site to indicate no archival copying by robots should take place constitutes an effective technological measure. Healthcare Advocates had filed a lawsuit alleging that a competitor infringed trademarks and copyrights and misappropriated trade secrets belonging to Healthcare Advocates. The defendants in that case were represented by the boutique IP law firm of Harding, Earley, Follmer & Frailey. To aid in preparing a defense, on two occasions employees of the Harding firm accessed screenshots of old versions of Healthcare Advocates' web sites that had been archived by the Internet Archive's web site (www.archive.org). The old versions of the web site were accessed through the "Wayback Machine," an information retrieval system offered to the public by the Internet Archive that allowed users to request archived screenshots contained in its archival database. Viewing the content that Healthcare Advocates had included on its public web site in the past was very useful to the Harding firm in assessing the merits of the trademark and trade secret allegations brought against the firm's clients.¹¹⁶³

The Internet Archive had a policy to respect robots.txt files and not to archive sites containing a robots.txt file that indicated the site should not be archived. In addition, for those web sites that did not have a robots.txt file present at the web site's inception, but included it later, the Internet Archive would remove the public's ability to access any previously archived screenshots stored in its database. The archived images were not deleted, but were instead rendered inaccessible to the general public, and the Internet Archive's web crawler was instructed not to gather screenshots of that web site in the future.¹¹⁶⁴

Healthcare Advocates had not included a robots.txt file on its web site prior to July 7, 2003. Consequently, Internet Archive's database included screenshots from Healthcare Advocates' web site when the Harding firm's employees accessed that database through the Wayback Machine on July 9, 2003 and July 14, 2003. On those two dates of access, however, the Internet Archive's servers, which checked for robots.txt files and blocked the images from being displayed from the corresponding web site, were malfunctioning due to a cache exhaustion condition. Because of this malfunction, employees of the Harding firm were able to view and print copies of the archived screenshots of Healthcare Advocates' web site stored in Internet Archive's database, contrary to Internet Archives' normal policy. Healthcare Advocates sued the Harding firm, alleging that it has manipulated the Wayback Machine on the two dates in question in a way that rendered useless the protective measure of the robots.txt file that

¹¹⁶² 2007 U.S. Dist. LEXIS 52544 (E.D. Pa. July 20, 2007).

¹¹⁶³ *Id.* at *1-3.

¹¹⁶⁴ *Id.* at *7-8.

Healthcare Advocates had placed on its web site, in violation of the anti-circumvention provisions of the DMCA.¹¹⁶⁵

The court turned first to the question of whether the robots.txt file used by Healthcare Advocates qualified as a technological measure effectively controlling access to its web site as defined in the Section 1201(a)(3)(B) of the DMCA. The court concluded on the particular facts of the case that it did, although the court refused to hold that a robots.txt file universally constitutes a technological protection measure:

The measure at issue in this case is the robots.txt protocol. No court has found that a robots.txt file universally constitutes a “technological measure effectively controll[ing] access” under the DMCA. The protocol by itself is not analogous to digital password protection or encryption. However, in this case, when all systems involved in processing requests via the Wayback Machine are operating properly, the placement of a correct robots.txt file on Healthcare Advocates’ current website does work to block users from accessing archived screenshots on its website. The only way to gain access would be for Healthcare Advocates to remove the robots.txt file from its website, and only the website owner can remove the robots.txt file. Thus, in this situation, the robots.txt file qualifies as a technological measure effectively controlling access to the archived copyrighted images of Healthcare Advocates. This finding should not be interpreted as a finding that a robots.txt file universally qualifies as a technological measure that controls access to copyrighted works under the DMCA.¹¹⁶⁶

However, the court found no violation of the DMCA by the actions of the Harding firm employees because those employees had not acted to “avoid” or “bypass” the technological measure. The court noted that those choice of words in the DMCA “imply that a person circumvents a technological measure only when he affirmatively performs an action that disables or voids the measure that was installed to prevent them from accessing the copyrighted material.”¹¹⁶⁷ The employees of the Harding firm had not taken such affirmative action. As far as they knew, no protective measures were in place with respect to the archived screenshots they were able to view, and they could in fact not avoid or bypass any protective measure because on the dates in question nothing stood in the way of them viewing the screenshots.¹¹⁶⁸

Healthcare Advocates argued that liability under the DMCA should be judged on what the Harding firm knew, not what actions it took. Healthcare Advocates argued that the Harding firm knew it was not permitted to view certain archived images, because some of the images were blocked. Healthcare Advocates therefore claimed that the firm knew or should have known that it was not supposed to be able to view any of the screenshots at issue, and that any request

¹¹⁶⁵ *Id.* at *4, *8-10 & *43.

¹¹⁶⁶ *Id.* at *41-42 (citation omitted).

¹¹⁶⁷ *Id.* at *46.

¹¹⁶⁸ *Id.* at *47.

made for archived images after the first request resulted in a denial constitute circumvention of its robots.txt file. The court rejected this argument, ruling that simply making further requests is not circumvention under the DMCA. The requests did not alter any computer code to render the robots.txt file void. Internet Archive's servers indicated that no lock existed when the requests were made. Accordingly, the Harding firm could not avoid or bypass a digital wall that was not there.¹¹⁶⁹

The court also ruled that Healthcare Advocates' inference that the Harding firm should have known it was not allowed to view any archived images via the Wayback Machine was both unreasonable and irrelevant. When a screenshot was blocked, the Wayback Machine returned a message stating that the page was blocked by the web site owner, but the message also included links, one of which said, "Try another request or click here to search for all pages on healthcareadvocates.com." When this page appeared, the firm's employee clicked on the link and received a list of all available screenshots.¹¹⁷⁰ The court held that, even if the firm knew that Healthcare Advocates did not give it permission to see its archived screenshots, "lack of permission is not circumvention under the DMCA."¹¹⁷¹ Accordingly, the court granted the Harding firm summary judgment on Healthcare Advocates' claim of a violation of the DMCA.¹¹⁷²

(iii) Apple v. Psystar

The facts of this case are set forth in Section II.G.1(b)(14) above. The court rejected the defendant's argument that Apple's encryption of its Mac OS X operating system files, which were decrypted by a decryption key stored within Apple's hardware, was not an effective technological protection measure because the decryption key was publicly available on the Internet. "The fact that circumvention devices may be widely available does not mean that a technological measure is not, as the DMCA provides, effectively protecting the rights of copyright owners in the ordinary course of its operations."¹¹⁷³

(iv) Ticketmaster v. Prestige Entertainment

In Ticketmaster L.L.C. v. Prestige Entertainment, Inc.,¹¹⁷⁴ Ticketmaster brought a claim under Section 1201(a) against the defendants for the use of bots to circumvent Ticketmaster's CAPTCHA and other security measures so as to be able to purchase large quantities of tickets on Ticketmaster's site. The defendants used colocation facilities with high speed bandwidth, random number and letter generators, and other evasive methods in order to avoid detection by

¹¹⁶⁹ Id. at *47-50.

¹¹⁷⁰ Id. at *50-51.

¹¹⁷¹ Id. at *51.

¹¹⁷² Id.

¹¹⁷³ Apple, Inc. v. Psystar Corp., 673 F. Supp. 2d 931, 942 (quoting Sony Computer Entm't Am., Inc. v. Divineo, Inc., 457 F. Supp. 2d 957, 965 (N.D. Cal. 2006)).

¹¹⁷⁴ 306 F. Supp. 3d 1164 (C.D. Cal. 2018).

Ticketmaster. The defendants brought a motion to dismiss the Section 1201(a) claim, arguing that the CAPTCHA and “splunk” measures (unique identifiers for ticket purchasers used to determine if users were exceeding purchase limits) used by Ticketmaster were not technological measures as defined in the DMCA.¹¹⁷⁵

The court denied the motion, noting that because a CAPTCHA prevents a user from proceeding further to gain access to copyrighted pages, it qualifies as a technological measure that effectively controls access to a copyrighted work. By using bots or “CAPTCHA farms,” the defendants were avoiding CAPTCHA without the authority of Ticketmaster. The fact that legitimate users could complete a CAPTCHA in an identical manner was irrelevant, because legitimate users did so with the authority of Ticketmaster. The court also ruled that whether a method of circumvention has innocent uses is irrelevant because Section 1201(a) is concerned with the circumvention itself, not the method. The defendants’ use of colocation facilities and other methods, such as deleting tracking tools like cookies, were also actionable under the DMCA if used to circumvent Ticketmaster’s technological measures.¹¹⁷⁶

Shortly after the court’s decision, Ticketmaster filed an amended complaint and the defendants again moved to dismiss it in its entirety, including the Section 1201(a) claims. The court noted that the amended complaint did contain new factual allegations, but none of them disturbed the sufficiency of the plaintiff’s DMCA claim. The defendants’ main argument was that Ticketmaster failed to indicate any copyrighted work to which any of Ticketmaster’s technological measures were effectively controlling access. The court ruled that such argument failed because Ticketmaster’s CAPTCHA controlled access to Ticketmaster’s ticket purchase pages and ticket confirmation pages so that only a human could progress through Ticketmaster’s pages and ultimately purchase a ticket. Each of the pages presented to the human customer was a unique page, tailored specifically to the customer and what that customer was trying to accomplish. When the defendants used bots to progress through Ticketmaster’s security measures and ultimately gain access to ticket confirmation pages and data, they circumvented a technological measure that Ticketmaster had put in place to control access to those pages and data, which were protected by copyright as dynamic non-literal content and literal content of the web site, respectively. The court noted that its holding comported with the growing number of courts to have concluded that circumvention of CAPTCHA and similar measures designed to distinguish between humans and non-humans violates the DMCA. Accordingly, the court denied the defendants’ motion to dismiss the plaintiff’s circumvention claim.¹¹⁷⁷

(v) Philips N. Am. v. Summit Imaging

The plaintiff Philips manufactured and sold ultrasound imaging devices that included certain software and hardware features that could be used only when Philips enabled a particular licensable feature for the specific ultrasound system based on what features a

¹¹⁷⁵ Id. at 1169-70, 1174.

¹¹⁷⁶ Id. at 1174.

¹¹⁷⁷ Ticketmaster L.L.C. v. Prestige Entm’t West, Inc., 315 F. Supp. 3d 1147, 1154 & 1166-67 (C.D. Cal. 2018).

customer had purchased. Philips alleged that the defendant hacked into Philips' software and altered the ultrasound systems using a computer program it developed called Adepto so as to enable features or options for which Philips' customers had not paid. Philips brought claims under Sections 1201(a)(1) and (a)(2). The defendants moved to dismiss the claims for failure to allege sufficient facts supporting that a technological measure that effectively controlled access to a copyrighted work had been circumvented.¹¹⁷⁸

The court denied the motion, noting that the complaint identified the following six layers of technological controls that Philips employed on its ultrasound systems to protect its copyrighted works from unauthorized access: (1) user-specific codes; (2) user-specific hardware keys; (3) machine-specific codes and hardware keys; (4) software files with licensed features and optional add-on controls; (5) machine-specific configuration files that controlled compatibility between the systems and software and/or the systems and replacement parts; and (6) software disabling if a user attempted to make use of an unlicensed feature. The user-specific access codes and hardware keys enabled the software access and control features for a particular registered user by permitting access to enabled Philips tools and features based on a user's registered access authorization level. The machine-specific controls permitted user access only to the features and tools that had been enabled on a specific machine. And the licensed feature controls limited what features users could access on a specific machine, controlled access to protected software, and limited the options available for use on a specific machine. These allegations were sufficient to plead that Philips' ultrasound system were protected by a technological measure that effectively controlled access to a copyrighted work.¹¹⁷⁹

The court also determined that Philips had adequately alleged that the defendants took actions to circumvent Philips' access controls. Philips alleged that the defendants removed the hard drive from the ultrasound systems and ran the Adepto program in order to change configuration files and software files so as to enable unlicensed options on the hard drive. Philips also alleged that the defendants used Adepto to hack onboard tools to force compatibility with otherwise incompatible transducer parts. The court ruled these allegations sufficiently alleged circumvention and therefore denied the defendants' motion.¹¹⁸⁰

(4) Whether Unauthorized Use of a Valid Password or Key Constitutes Circumvention

(i) Cases Holding That It Does Constitute Circumvention

a. 321 Studios v. Metro Goldwyn Mayer

This case is discussed in Section II.G.1(a)(13)(viii) below.

¹¹⁷⁸ Philips N. Am., LLC v. Summit Imaging Inc., 2020 U.S. Dist. LEXIS 55073 at *1-3, *6 (W.D. Wa. Mar. 30, 2020).

¹¹⁷⁹ Id. at *8-9.

¹¹⁸⁰ Id. at *10-11.

b. Microsoft v. EEE Business

In this case, the defendant engaged in the unauthorized distribution of Microsoft software that was available only under a Volume License Agreement. The agreement permitted only authorized volume licensees to install software to unlock the media programming to enable the user to enter a 25-character alphanumeric code, called the Volume License Key (VLK), which was unique to the licensee and required to be kept confidential under the terms of the Volume License Agreement. The court ruled that, by distributing a VLK without authorization, the defendant had effectively circumvented Microsoft's technological measure to control access to a copyrighted work in violation of Section 1201(a)(2) of the DMCA.¹¹⁸¹

c. Actuate v. IBM

In Actuate Corp. v. International Business Machines Corp.,¹¹⁸² Actuate alleged that IBM's unauthorized posting on an IBM web site of Actuate's copyrighted software for downloading, together with the license keys that allowed for unlimited use of such software by downloaders, whether they were authorized to use the software or not, constituted circumvention of technological measures on the software that restricted access to it and trafficking in circumvention devices. IBM filed a motion to dismiss the claim, relying on the I.M.S., Egilman, and R.C. Olmstead cases for the proposition that improper use of a legitimate password issued by the copyright holder does not constitute circumvention.¹¹⁸³

The court denied the motion. It found the I.M.S., Egilman, and R.C. Olmstead cases in conflict with the 321 Studios and the Microsoft v. EEE Business cases from the Northern District of California with respect to the issue of whether the unauthorized use of an otherwise legitimate password can constitute circumvention. The court rejected IBM's argument that the two lines of cases were not inconsistent on the ground that, in the 321 Studios and Microsoft v. EEE Business cases, there was no allegation that the parties whose passwords were being used had issued those passwords to a third party. The court found no basis in 321 Studios for such a distinction, and noted that Egilman expressly rejected the distinction. Accordingly, the court concluded that the two lines of cases simply reached contradictory results, and declined to follow the reasoning of the I.M.S. line of cases. It instead followed the 321 Studios and the Microsoft v. EEE Business cases, and held that unauthorized distribution of passwords and user-names avoids and bypasses a technological measure in violation of Sections 1201(a)(2) and 1201(b)(1).¹¹⁸⁴

The reasoning of the I.M.S. court – that a password somehow does not fall within [the analogy to the combination of a locked door used in the DeCSS cases], is not well-founded. Rather, a combination to a lock appears to be essentially the same as a

¹¹⁸¹ Microsoft Corp. v. EEE Business Inc., 555 F. Supp. 2d 1051, 1059 (N.D. Cal. 2008).

¹¹⁸² 2010 U.S. Dist. LEXIS 33095 (N.D. Cal. Apr. 5, 2010).

¹¹⁸³ Id. at *9-10.

¹¹⁸⁴ Id. at *24-25.

password. Nor does the Court find support in the statute itself for drawing a distinction between passwords and other types of code that might be used for decryption. Therefore, the Court rejects Defendants’ position. Unauthorized use of a password may constitute circumvention under the DMCA.¹¹⁸⁵

(ii) Cases Holding That It Does Not Constitute Circumvention

a. I.M.S. Inquiry Management Systems v. Berkshire Management Systems

This case reached the opposite result from the 321 Studios v. Metro Goldwyn Mayer case (discussed in Section II.G.1(a)(13)(viii) below), and held that the unauthorized use of an otherwise legitimate, owner-issued password does not constitute a “circumvention” of a technological measure under the DMCA.¹¹⁸⁶ The plaintiff owned a web-based service that provided information on tracking magazine advertising exclusively to its clients through proprietary passwords. The defendant obtained a user identification and password issued to a third party and made unauthorized use of the same to gain access to the plaintiff’s web site, from which the defendant downloaded approximately 85% of the report formats and copied those formats into its competing service.¹¹⁸⁷ The court ruled there was no DMCA violation because “what defendant avoided and bypassed was *permission* to engage and move through the technological measure from the measure’s author. ... Defendant did not surmount or puncture or evade any technological measure to do so; instead, it used a password intentionally issued by plaintiff to another entity.”¹¹⁸⁸

b. Egilman v. Keller & Heckman

¹¹⁸⁵ Id. at *26. Accord Synopsys, Inc. v. Innogrit, Corp., 2019 U.S. Dist. LEXIS 171487 (N.D. Cal. Oct. 1, 2019) (citing Actuate, holding that unauthorized use of license keys or passwords constitutes circumvention under Section 1201(a)(1)). In an earlier decision, the court granted a preliminary injunction to Synopsys based on likelihood of success on the merits of (1) claims under Section 1201(a)(1) where forensic evidence collected from the defendant’s computers revealed evidence of software piracy, including forensic artifacts related to counterfeit license keys, counterfeit key generators, and “crack” files for Synopsys software containing tools to unlock unauthorized copies of Synopsys software, as well as evidence showing the defendant manually changed the media access control (MAC) addresses on 11 computers in the U.S., which allowed the defendant to run Synopsys software on unauthorized computers; and on claims under Section 1201(a)(2) where forensic evidence showed that the defendant imported a crack file from an Iranian software piracy web site and obtained license key generator software from a Chinese web site known to host pirated software. Synopsys, Inc. v. InnoGrit, Corp., 2019 U.S. Dist. LEXIS 107215 at *6-7 (N.D. Cal. June 26, 2019).

¹¹⁸⁶ I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc., 307 F. Supp. 2d 521 (S.D.N.Y. 2004).

¹¹⁸⁷ Id. at 523.

¹¹⁸⁸ Id. at 532-33.

This case agreed with the I.M.S. case and held that access to a computer through the unauthorized use of a valid password does not constitute an unlawful circumvention.¹¹⁸⁹ The plaintiff Egilman was a medical doctor and testifying expert witness in a case in which the court had issued an order prohibiting anyone involved in the litigation from publishing any statements on Internet websites over which they had control concerning the litigation. Egilman was sanctioned for violating the order by publishing certain inflammatory statements on his website. Egilman claimed that one of the defendant's law firms had obtained the user name and password to his website without authorization and disclosed that information to another defendant's law firm, which then used the user name and password to gain access to his website, from which the firm obtained information showing that Egilman had violated the court order. Egilman asserted a claim under the anti-circumvention provisions against the law firm.¹¹⁹⁰

The court rejected the claim. It reviewed the facts and holding of the I.M.S. case discussed in subsection j. above, and found that the case was correctly decided.¹¹⁹¹ The court therefore ruled that "using a username/password combination as intended – by entering a valid username and password, albeit without authorization – does not constitute circumvention under the DMCA." The "technological measure" employed by Egilman had not been "circumvented," but rather merely utilized.¹¹⁹²

c. R.C. Olmstead v. CU Interface

This case agreed with the I.M.S. case and held that access to a computer through the unauthorized use of a valid username and password does not constitute an unlawful circumvention.¹¹⁹³ The plaintiff was the owner of data processing software for credit unions called RCO-1 that it licensed to the defendant. The defendant CUI hired some developers to develop a replacement program for RCO-1 and, to aid development, allowed the developers to gain access to RCO-1 using valid usernames and passwords issued to CUI. The plaintiff claimed that such unauthorized access violated the DMCA. The court rejected this claim, finding the case indistinguishable from I.M.S. and the reasoning of I.M.S. persuasive. The court also noted that the license agreement between the plaintiff and CUI did not set any restrictions regarding issuance of usernames and passwords, so that the plaintiff could not even show that CUI's use of its usernames and passwords was unauthorized.¹¹⁹⁴ "Simply put, CUI did not circumvent or bypass any technological measures of the RCO software – it merely used a username and password – the approved methodology – to access the software."¹¹⁹⁵

¹¹⁸⁹ Egilman v. Keller & Heckman, LLP, 401 F. Supp. 2d 105 (D.D.C. 2005).

¹¹⁹⁰ Id. at 107-09.

¹¹⁹¹ Id. at 112-14.

¹¹⁹² Id. at 114.

¹¹⁹³ R.C. Olmstead, Inc. v. CU Interface, LLC, 2009 U.S. Dist. LEXIS 87705 (N.D. Ohio Mar. 27, 2009).

¹¹⁹⁴ Id. at *21-24.

¹¹⁹⁵ Id. at *24.

d. Navistar v. New Baltimore Garage

In this case, the plaintiff restricted access to its dealer communication network and copyrighted material stored therein through use of passwords. The license agreement for use of the network prohibited sharing with or otherwise distributing passwords to third parties and using a third party's password to gain access to the network. The defendant, a licensee of the plaintiff's network, violated these prohibitions and shared its passwords with a third party who used them to log in and gain unauthorized access to information on the plaintiff's network. The plaintiff claimed that the defendant's provision to the third party with access to the plaintiff's network through the unauthorized use of its passwords constituted circumvention of a technological measure or trafficking in technology designed to circumvent access or copy controls. The court, noting a split in authority on the issue, ruled that unauthorized use of a valid password does not violate the anti-circumvention provisions of the DMCA, and the unauthorized sharing of a valid password does not constitute prohibited trafficking. Accordingly, the court granted the defendant's motion to dismiss the plaintiff's DMCA claim with leave to amend.¹¹⁹⁶

e. Digital Drilling Data Sys. v. Petrolink

This case is discussed in Section II.G.1(a)(1)(xvii) above.

f. R. Christopher Goodwin & Assocs. v. Search, Inc.

The plaintiff claimed that an employee of the defendant, Dr. Pevny, accessed and downloaded copyrighted material stored on the plaintiff's computer server after she had already accepted an employment offer from the defendant. The plaintiff asserted violations of Section 1201 on the ground that, although Dr. Pevny had access to the secured computer, her authorization was limited to access and use of the copyrighted files for exclusive use in the course and scope of her employment with the plaintiff. The plaintiff alleged that by downloading files after having tendered her resignation, Dr. Pevny exceeded her authorization and violated Section 1201. The court ruled that these allegations did not state a claim for circumvention under Section 1201. The court noted that circumvention is an essential part of a violation. While the user id/password combination required for access was a technological measure that controlled access to the works at issue, Dr. Pevny did not circumvent that measure. She validly accessed the system using her id/password combination while she was still an employee with the plaintiff. Her alleged abuse of her logon privileges did not rise to the level of descrambling, decrypting, or otherwise avoiding, bypassing, removing, deactivating, or impairing anything.¹¹⁹⁷ The court cited several district court cases for the proposition that using the correct username and password to access a copyrighted work, even without authorization to do so, does not

¹¹⁹⁶ Navistar, Inc. v. New Baltimore Garage, Inc., 2012 U.S. Dist. LEXIS 134369 at *2-5, *13-15 & *29 (N.D. Ill. Sept. 20, 2012).

¹¹⁹⁷ Christopher Goodwin & Assocs. v. Search, Inc., 2019 U.S. Dist. LEXIS 187073 at *2, *6-7 (E.D. La. Oct. 29, 2019).

constitute circumvention under Section 1201.¹¹⁹⁸ The court therefore granted the defendant's motion to dismiss the Section 1201 claim.¹¹⁹⁹

(iii) Cases Refusing to Decide the Issue

a. Avaya v. Telecom Labs

In this case, the court refused to decide on a motion for summary judgment the issue addressed in the I.M.S. case of whether unauthorized use of a valid password to gain access to software constitutes a violation of the DMCA.¹²⁰⁰ The plaintiff Avaya sold PBX systems with maintenance software embedded in them. When selling a new system, Avaya supplied the customer with a set of default passwords that the customer used to first log in to the system. Avaya alleged that the passwords were used without authorization by the defendants to log in and gain access to Avaya's maintenance software. Defendants moved for summary judgment that use of valid logins to gain access to software does not violate the DMCA. The court ruled that summary judgment was not appropriate because granting the motion would not result in dismissal of any portion of Avaya's DMCA claims from the case. All that would be resolved would be the abstract issue of whether use of valid logins does not violate the DMCA. Because Avaya had not identified a single, specific PBX to which the alleged illegal conduct was applied, ruling on the motion would have no effect until such time as the defendants could prove which of the PBXs at issue were accessed with the known, valid logins that they alleged were immune from DMCA liability.¹²⁰¹ "Avaya's DMCA claims may or may not have merit, but a summary judgment rendered on a discrete set of facts that have yet to be proven is not the proper vehicle for that determination."¹²⁰²

(5) No Requirements With Respect to Design of a Product; Other Rights

Not Affected

Section 1201(c)(3) provides that nothing in the bills "shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure"

Sections 1201(c)(1), (2), and (4) provide that Section 1201 is not intended to affect rights, remedies, limitations, or defenses (including fair use) to copyright infringement; or to enlarge or diminish vicarious or contributory liability in connection with any technology or product; or to

¹¹⁹⁸ Id. at *7-8 (citing the I.M.S. and Egilman cases discussed in Sections II.G.1(a)(4)(ii).a and .b above, and Joint Stock Co. Channel One Russia Worldwide v. Infomir LLC, 2017 U.S. Dist. LEXIS 22548 at *18 (S.D.N.Y. Feb. 15, 2017)).

¹¹⁹⁹ Id. at *8.

¹²⁰⁰ Avaya, Inc. v. Telecom Labs, Inc., 2009 U.S. Dist. LEXIS 82609 (D.N.J. Sept. 9, 2009).

¹²⁰¹ Id. at *2 & *10-13.

¹²⁰² Id. at *13.

enlarge or diminish any rights of free speech of the press for activities using consumer electronics, telecommunications, or computing products.

Notwithstanding these provisions, groups such as the Digital Future Coalition (DFC) have criticized the approach of the DMCA. In a position paper dated August 1997,¹²⁰³ the DFC argued that Section 1201 would effectively negate fair use rights, because it imposes liability for “circumvention” even when the purpose of the activity is permitted by the copyright act (such as reverse engineering or other activities that otherwise constitute fair use). The DFC also argued that Section 1201 would outlaw legitimate devices with substantial noninfringing uses, effectively overruling the Supreme Court’s decision in Sony Corp. v Universal City Studios.¹²⁰⁴

The DFC argued that the savings clauses of Section 1201(c) are inadequate because “while Section 1201 will not as a formal matter restrict existing limitations and exceptions to copyright, it will as a practical matter preclude the exercise of these limitations and exceptions by preventing the manufacture and use of the technologies necessary for their existence. Nor would the savings clause protect individuals who gain ‘access’ to works in violation of 1201(a)(1), even if they do so for entirely lawful purposes.”¹²⁰⁵

Another position paper filed on behalf of the Information Technology Industry Council raised concern that Section 1201 will impose liability too broadly in view of the broad definition of “circumvention”:

Thus, if a device does not respond to a technological protection measure that is intended to control copying, which in some cases may be a simple 1 or 0 in header information included with the digital content, the device may be construed as avoiding, bypassing, deactivating or impairing that measure.... Companies that make devices that do not respond to copy flags – because they don’t know about the flags or because of technological difficulties associated with complying – could be liable under Section 1201 even though they had no intent to circumvent.¹²⁰⁶

The paper also raised concern about broadening the standard for liability for third party use of devices that infringe copyright owner’s rights from that of the Sony case, which imposes liability only for sale of devices having no substantial noninfringing uses, to the prohibition under the bill of devices that are “primarily designed or produced” for circumvention, or have “only

¹²⁰³ The position paper may be found at www.ari.net/dfc/docs/stwip.htm.

¹²⁰⁴ 464 U.S. 417 (1984).

¹²⁰⁵ Position paper at 3.

¹²⁰⁶ Prepared Statement of Chris Byrne of Silicon Graphics, Inc. on Behalf of the Information Technology Industry Council Before the House Judiciary Committee Courts and Intellectual Property Subcommittee (Wed., Sept. 17, 1997) (available from Federal News Service, 620 National Press Building, Washington, D.C. 20045, and on file with the author). Section 1201(c)(3), discussed above, appears to be directed at least in part to addressing this issue.

limited commercially significant purpose” other than circumvention, or are marketed for use in circumvention.

(6) Exemption for Nonprofit Organizations and Law Enforcement

Section 1201(d) sets up an exemption from the circumvention prohibitions of Section 1201(a)(1) for nonprofit libraries, archives, or educational institutions that gain access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work, provided that a copy of the work is not retained longer than necessary to make the good faith determination, is used for no other purpose, and there is not otherwise reasonably available an identical copy of the work in another form. Section 1201(e) provides that the prohibitions of Section 1201 do not apply to lawfully authorized investigative, protective, information security,¹²⁰⁷ or intelligence activity of law enforcement officers.

(7) Reverse Engineering for Interoperability

Section 1201(f) provides three exemptions to the anti-circumvention provisions relating to reverse engineering and interoperability:

Reverse Engineering for Interoperability of an Independently Created Computer Program. Section 1201(f)(1) provides that, notwithstanding the prohibitions in Section 1201(a)(1)(A), “a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.” The language in Section 1201(f) requiring that the reverse engineering be for the sole purpose of “identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs” comes directly from Article 6 of the European Union Software Directive, and appears to be the first time that language from an EU Directive has been incorporated verbatim into the United States Code.¹²⁰⁸

Development and Employment of a Technological Means for Enabling Interoperability. Section 1201(f)(2) provides that, notwithstanding the prohibitions in Sections 1201(a)(2) and 1201(b), “a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable

¹²⁰⁷ Section 1201(e) defines “information security” to mean activities carried out to identify and address the vulnerabilities of a government computer, computer system, or computer network.

¹²⁰⁸ Jonathan Band & Taro Issihiki, “The New Anti-Circumvention Provisions in the Copyright Act: A Flawed First Step,” *Cyberspace Lawyer*, Feb. 1999, at 2, 4. Section 1201(f) may also represent the first Congressional recognition of the legitimacy of software reverse engineering. *Id.*

the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title.”

The scope of this exemption is uncertain from its language in several respects. First, it is unclear what kinds of “technological means” Congress had in mind for falling within this exemption. The reference to allowing a person to “develop *and* employ” such technological means may suggest that the exemption is limited to only those means developed by the person desiring to circumvent, as opposed to commercially available circumvention means. The legislative history suggests otherwise, however, for it contemplates that the rights under Section 1201(f)(2) may be exercised through either generally available tools or specially developed tools:

[Section 1201(f)(2)] recognizes that to accomplish the acts permitted under [Section 1201(f)(1)] a person may, in some instances, have to make and use certain tools. In most instances these will be generally available tools that programmers use in developing computer programs, such as compilers, trace analyzers and disassemblers, which are not prohibited by this section. In certain instances, it is possible that a person may have to develop special tools to achieve the permitted purpose of interoperability. Thus this provision creates an exception to the prohibition on making circumvention tools contained in subsections 1201(a)(2) and (b). These tools can be either software or hardware.¹²⁰⁹

From this legislative history, it is apparent that the phrase “develop and employ” in Section 1201(f)(2) was probably intended to mean “develop and/or employ.”

A second ambiguity is whether the “technological means” of Section 1201(f)(2) were intended to be limited to the kinds of reverse engineering “tools” cited in the legislative history (compilers, trace analyzers, disassemblers and the like), or whether they could be read more broadly to encompass computer programs, such as application programs, that in their ordinary operation are designed to circumvent technological measures protecting another computer program so as to interoperate with it. For example, consider the fact pattern at issue in the case of Lexmark International, Inc. v. Static Control Components, Inc.,¹²¹⁰ discussed in Section II.G.1(o)(1) below. In that case, the district court ruled on a motion for a preliminary injunction that Static Control violated Section 1201(a)(2) by distributing microchips that were used to replace the microchip found in the plaintiff Lexmark’s toner cartridges. Static Control’s microchip contained a computer program that circumvented Lexmark’s authentication sequence that prevented the printer engine software on the Lexmark printer from allowing the printer to operate with a refilled toner cartridge.

¹²⁰⁹ S. Rep. No. 105-190, at 33 (1998).

¹²¹⁰ 253 F. Supp. 2d 943, 948-49 (E.D. Ky. 2003), rev’d, 387 F.3d 522 (6th Cir. 2004), reh’g denied, 2004 U.S. App. LEXIS 27422 (Dec. 29, 2004), reh’g en banc denied, 2005 U.S. App. LEXIS 3330 (6th Cir. Feb. 15, 2005).

The district court in that case ruled that the exemptions of Section 1201(f) did not apply because Static Control's microchips could not be considered to contain independently created computer programs, since the toner loading program on those microchips was an exact copy of the toner loading program contained on Lexmark's microchips.¹²¹¹ However, suppose Static Control had independently developed the computer program contained on its microchips.¹²¹² Would the exemption of Section 1201(f)(2) apply? Static Control could argue yes, on the ground that Section 1201(f)(2) permits it to "employ technological means [the computer program on its microchip] to circumvent a technological measure [the authentication sequence implemented by the Lexmark printer engine software] ... for the purpose of enabling interoperability of an independently created computer program [again, the computer program on Static Control's microchip] with other programs [the Lexmark printer engine program]."

On the other hand, Lexmark could argue no, on the ground that the legislative history indicates that the "technological means" referenced in Section 1201(f)(2) were meant to be limited to reverse engineering "tools," and the program on the Static Control microchip is not a reverse engineering tool, but rather an application program. In sum, the issue is whether the "independently created computer program" referenced in Section 1201(f)(2) can also constitute the "technological means" of circumvention, or whether the "technological means" is limited to the reverse engineering tool used to develop the independently created computer program in the first place. Stated differently, the issue is whether Section 1201(f)(2) was meant to be narrow to cover only the development and employment of special tools used to aid the reverse engineering permitted by Section 1201(f)(1), or whether it was intended to permit more generalized circumvention of technological measures by one computer program in order to interoperate with another computer program whose technological protection measures are being circumvented by the first program. A similar ambiguity is embedded in Section 1201(f)(2)'s reference to "other" programs – can a program whose technological measure is circumvented by an independently created computer program, both in the ordinary operation of the independently created computer program and in the reverse engineering that was done to create such program, qualify as an "other" program? The legislative history contains no guidance on the interpretation of "other" in the exemption.

It appears that the Copyright Office agrees with an expansive reading of the Section 1201(f) exemption. After the district court's decision in the Lexmark case came down, Static

¹²¹¹ As discussed further in Section II.G.1(a)(13)(i) below, the Sixth Circuit on appeal reversed the district court's grant of a preliminary injunction and remanded. Among other things, the Sixth Circuit questioned whether Lexmark's toner loading program was even copyrightable, ruling that on the preliminary injunction record Lexmark had made inadequate showings with respect to originality of its toner loading program and whether that program functioned as a "lock-out code" that had to be copied for functional purposes. Lexmark Int'l v. Static Control Components, 387 F.3d 522, 536-41 (6th Cir. 2004), reh'g denied, 2004 U.S. App. LEXIS 27422 (Dec. 29, 2004), reh'g en banc denied, 2005 U.S. App. LEXIS 3330 (6th Cir. Feb. 15, 2005).

¹²¹² The Sixth Circuit also ruled that, whether or not the toner loading program on Static Control's microchips was independently created, the record established that there were other programs on Static Control's microchips that were independently created, and those computer programs also interoperated with Lexmark's printer engine program on Lexmark's microchips. Id. at 550.

Control submitted a proposed exemption to the Copyright Office in its 2003 rulemaking proceeding under Section 1201(a)(1) to determine classes of works exempt from the anti-circumvention prohibitions. In particular, Static Control asked for an exemption for the following classes of works:

1. Computer programs embedded in computer printers and toner cartridges and that control the interoperation and functions of the printer and toner cartridge.
2. Computer programs embedded in a machine or product and which cannot be copied during the ordinary operation or use of the machine or product.
3. Computer programs embedded in a machine or product and that control the operation of a machine or product connected thereto, but that do not otherwise control the performance, display or reproduction of copyrighted works that have an independent economic significance.¹²¹³

The Copyright Office set forth its analysis of Static Control's requested exemptions, among many other requested exemptions, in a lengthy memorandum issued on Oct. 27, 2003 by the Register of Copyrights to the Librarian of Congress. Although it is not clear from the memorandum whether the Copyright Office took a position with request to Static Control's second and third proposed exemptions, the Copyright Office determined that no exemption was warranted for the first proposed exemption because "Static Control's purpose of achieving interoperability of remanufactured printer cartridges with Lexmark's ... printers could have been lawfully achieved by taking advantage of the defense found in §1201(f), the reverse engineering exemption."¹²¹⁴

The Copyright Office read the purpose behind Section 1201(f) broadly: "Not only did Congress intend that 'interoperability' include the exchange of information between computer programs; it also intended 'for such programs mutually to use the information which has been exchanged.' Interoperability necessarily includes, therefore, concerns for functionality and use, and not only of individual use, but for enabling competitive choices in the marketplace."¹²¹⁵ The Copyright Office elaborated that the statutory exemptions of Section 1201(f) afford broader exemptions than even the Copyright Office itself could grant by virtue of rulemaking. In particular, the Copyright Office's exemptions are limited to individual acts of exemption prohibited by Section 1201(a)(1), whereas the statutory exemptions of Section 1201(f) include the distribution of the means of circumvention into the marketplace:

¹²¹³ Memorandum from Marybeth Peters, Register of Copyrights, to James H. Billington, Librarian of Congress, "Recommendation of the Register of Copyrights in RM 2002-4; Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies," Oct. 27, 2003, p. 172, available as of Jan. 10, 2004 at www.copyright.gov/1201/docs/registers-recommendation.pdf.

¹²¹⁴ *Id.* at 176.

¹²¹⁵ *Id.* at 178 (quoting the House Manager's Report at 14).

[T]he statutory exemption found in §1201(f) not only permits circumvention of technological measures to analyze and identify interoperable elements of a protected computer program, but also provides exemptions to the trafficking provisions in §1201(a)(2) and 1201(b). Even if the Register had found a factual basis for an exemption, it would only exempt the act of circumvention. It would not exempt the creation and distribution of the means to circumvent or the distribution of interoperable computer programs embedded in devices. Since it is clear that Static Control’s goal was not merely to privately circumvent, but rather to facilitate the distribution of competitive toner cartridges to others, a recommendation for an exemption in this rulemaking would have little effect on the intended use.¹²¹⁶

Accordingly, the Copyright Office concluded that “Congress has comprehensively addressed the important concern of interoperability for competition and functionality within its own statutory exemption” and that an exemption through rulemaking was not necessary.¹²¹⁷

Providing Information or Means for Interoperability to Others. Section 1201(f)(3) provides that the “information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if the person referred to in paragraph (1) or (2), as the case may be, provides such information or means solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section.”

Section 1201(f)(3) contains ambiguities with respect to its scope that are similar to those noted with respect to Section 1201(f)(2). The legislative history for Section 1201(f)(3) states the following:

[Section 1201(f)(3)] recognizes that developing complex computer programs often involves the efforts of many persons. For example, some of these persons may be hired to develop a specific portion of the final product. For that person to perform these tasks, some of the information acquired through the permitted analysis, and the tools to accomplish it, may have to be made available to that person. This subsection allows developers of independently created software to rely on third parties either to develop the necessary circumvention tools or to identify the necessary information to achieve interoperability. The ability to rely on third parties is particularly important for small software developers who do not have the capability of performing these functions in-house. This provision permits such sharing of information and tools.¹²¹⁸

Although Section 1201(f)(3) clearly contemplates an exemption for distribution to third parties of the “technological means” referenced in Section 1201(f)(2), as well as the

¹²¹⁶ *Id.* at 180-81 (emphasis in original).

¹²¹⁷ *Id.* at 183.

¹²¹⁸ S. Rep. No. 105-190, at 33 (1998).

“information” gleaned from reverse engineering under Section 1201(f)(1), the same issues of the scope of “technological means” intended to be within the exemption arise as in Section 1201(f)(2). As noted, the Copyright Office seems to read Section 1201(f)(3) broadly to permit the distribution of independently developed computer programs that circumvent the technological protection measures of other programs in order to interoperate with such other programs. The legislative history quoted above, however, seems to read Section 1201(f)(3) more narrowly as directed to distribution of reverse engineering “tools” or information to third party developers who may be hired to assist in the development of an independent computer program, as opposed to a distribution of a competitive product into the marketplace.

These ambiguities in the scope of the Section 1201(f) exemptions will need to be resolved over time through litigation. In addition, it is worth observing that, although Section 1201(f) provides useful exemptions, it leaves open the issue of whether circumvention of access restrictions in order to perform reverse engineering for purposes other than interoperability, such as error correction, is prohibited. The Copyright Office’s exemption rulemaking procedures may afford a mechanism to further flesh out or clarify the Section 1201(f) exemptions.

Several cases have adjudicated the scope of the Section 1201(f) exemption:

(i) Universal City Studios Inc. v. Reimerdes

In Universal City Studios, Inc. v. Reimerdes,¹²¹⁹ discussed in further detail in Section II.G.1(m)(4) below, the court rejected the applicability of Section 1201(f) to the defendants’ posting on their Web site of, and posting links to, a descrambling computer program known as “DeCSS,” which circumvented the encryption of movies stored in digital form on a digital versatile disk (“DVD”) encoded with the industry standard Content Scramble System (“CSS”). The defendants argued that DeCSS had been created to further the development of a DVD player that would run under the Linux operating system, as there allegedly were no Linux-compatible players on the market at the time.¹²²⁰ They further contended that DeCSS was necessary to achieve interoperability between computers running the Linux operating system and DVDs, and that the exception of Section 1201(f) therefore applied.¹²²¹

The court rejected this argument for several reasons. First, Section 1201(f)(3) permits information acquired through reverse engineering to be made available to others only by the person who acquired the information, and the defendants did not themselves do any reverse engineering (DeCSS had been created by a third party). Even if the defendants had authored DeCSS, the court ruled that Section 1201(f)(3) would allow the dissemination only of information gleaned from the reverse engineering and solely for the purpose of achieving interoperability as defined in the statute (which was not the reason the defendants posted DeCSS), and not

¹²¹⁹ 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

¹²²⁰ Id. at 319.

¹²²¹ Id. at 320.

dissemination of the means of circumvention itself.¹²²² Second, the defendants could not claim that the sole purpose of DeCSS was to create a Linux DVD player, because DeCSS was developed on and ran under the Windows operating system, and could therefore decrypt and play DVD movies on Windows as well as Linux machines.¹²²³ In addition, in an earlier opinion, the court ruled that Section 1201(f) was inapplicable because the legislative history of the DMCA makes clear that Section 1201(f) permits reverse engineering of copyrighted computer programs only and does not authorize circumvention of technological systems that control access to other copyrighted works, such as movies.¹²²⁴

(ii) Storage Technology Corporation v. Custom Hardware Engineering & Consulting

This case rejected an assertion of a Section 1201(f) defense because the defendant's circumvention resulted in an infringing copy of the plaintiff's copyrighted program being made in RAM, and the Section 1201(f) defense exempts circumvention only if it does not result in copyright infringement. For a discussion of the details of the case, see Section II.G.1(o)(4) below.

(iii) Chamberlain Group, Inc. v. Skylink Technologies, Inc.

The facts of this case are set forth in Section II.G.1(o)(2) below. Although this case did not directly adjudicate the scope of the Section 1201(f) exemptions, the court made a few statements in dicta suggesting that Section 1201(f) acts to immunize interoperability from anti-circumvention liability. In that case, the Federal Circuit ruled that the anti-circumvention provisions of Section 1201 do not apply to all forms of circumvention to gain access to a work, but rather only to circumventions that facilitate some form of copyright infringement.¹²²⁵ The court reached this conclusion in part on the rationale that a broad interpretation of the anti-circumvention provisions to prohibit all forms of unauthorized access, whether or not protected copyright rights were thereby implicated, would be tantamount to "ignoring the explicit

¹²²² Id.

¹²²³ Id.

¹²²⁴ Universal City Studios Inc. v. Reimerdes, 82 F. Supp. 2d 211, 218 (S.D.N.Y. 2000) (citing S. Rep. No. 105-190 (1998) and H.R. Rep. 105-551 (II) (1998)). Section 1201(f) would seem applicable to the original reverse engineering that the developers of DeCSS engaged in, but the trickier issue dealt with by the court is whether it should apply to subsequent use of the DeCSS to gain access to copyrighted works stored on a DVD in order to play such works under the Linux operating system. Such access is for use of the work stored on the DVD (albeit in an interoperable way), whereas the exception speaks in terms of "identifying and analyzing" the copyrighted work to achieve interoperability. In addition, Section 1201(f) appears to be a defense only to the conduct of circumvention prohibited by Section 1201(a)(1), and not to the distribution of devices prohibited under Sections 1201(a)(2) and 1201(b). Because the court found that DeCSS is a device within the prohibition of Section 1201(a)(2), it was not subject to the exception of Section 1201(f).

¹²²⁵ Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178, 1195, 1203 (Fed. Cir. 2004), cert. denied, 161 L. Ed. 2d 481 (2005).

immunization of interoperability from anticircumvention liability under § 1201(f).¹²²⁶ This language, although dicta, characterizes the Section 1201(f) exemption very broadly.¹²²⁷

Another dictum by the court in connection with articulating its rationale for rejecting such a broad interpretation of anti-circumvention liability makes clear the court's belief that the anti-circumvention provisions should not be construed to prevent interoperability of computer programs:

Chamberlain's proposed construction would allow any manufacturer of any product to add a single copyrighted sentence or software fragment to its product, wrap the copyrighted material in a trivial "encryption" scheme, and thereby gain the right to restrict consumers' rights to use its products in conjunction with competing products. In other words, Chamberlain's construction of the DMCA would allow virtually any company to attempt to leverage its sales into aftermarket monopolies – a practice that both the antitrust laws and the doctrine of copyright misuse normally prohibit.¹²²⁸

(iv) Lexmark International, Inc. v. Static Control Components, Inc.

For a discussion of the applicability of the reverse engineering exception of Section 1201(f) in this case, see Section II.G.1(o)(1) below.

(v) Davidson Assocs. v. Internet Gateway

In this case, the plaintiff Davidson & Assocs., doing business as Blizzard Entertainment, owned the copyrights in several computer games. The games could be played in either a single-player mode or in an online multi-player mode called "Battle.net mode."¹²²⁹ Blizzard operated a 24-hour online gaming service known as the Battle.net service that allowed owners of certain Blizzard games to play those games against each other in Battle.net mode by linking together over the Internet through Battle.net servers. In addition to multi-player game play, Battle.net mode allowed users to chat with other potential players, to record wins and losses and save advancements in a password protected individual game account, and to set up private games on the Battle.net service to allow players to determine whom they wished to interact with on the Battle.net service.¹²³⁰ The court noted that these Battle.net mode features were "accessed from

¹²²⁶ Id. at 1200.

¹²²⁷ The court noted that it had no occasion to reach the argument, raised by an amicus, that Section 1201(f) should cover the defendant's actions in distributing a product that circumvented technological measures restricting access to the plaintiff's computer program so as to interoperate with it. Because Section 1201(f) is an affirmative defense, the court noted that it would become relevant only if the plaintiff could prove a prima facie case of anti-circumvention liability to shift the burden to the defendant, which the court ruled the plaintiff had ultimately failed to do. Id. at 1200 n.15.

¹²²⁸ Id. at 1201 (citations omitted).

¹²²⁹ Davidson & Assocs. v. Internet Gateway, 334 F. Supp. 2d 1164, 1168 (E.D. Mo. 2004).

¹²³⁰ Id.

within the games themselves,” which seems to mean that there was particular code within the Blizzard games that allowed them to operate in Battle.net mode and communicate with the Battle.net servers.¹²³¹

The Battle.net service was designed to prohibit access and use of Battle.net mode by unauthorized or pirated copies of Blizzard games. In particular, in order to log on to the Battle.net service and access Battle.net mode, the Blizzard games were designed to initiate an authentication sequence or “secret handshake” between the game and the Battle.net server based on the “CD Key” of the game, a unique sequence of alphanumeric characters that was printed on a sticker attached to the case in which each game was packaged. The game would pass the CD Key to the Battle.net server, which would verify its validity and determine whether the same CD Key was already being used by another game that was currently logged on to the server. If the CD Key was determined to be valid by the server and not already in use, the server would send a signal to the game allowing it to enter the Battle.net mode and to use the Battle.net gaming services.¹²³²

In order to install a copy of a Blizzard game, the user was required to click acceptance of a clickwrap license agreement that prohibited reverse engineering of the software and that required the user to agree to the Terms of Use of the Battle.net service, which prohibited emulation or redirection of the communication protocols used by Blizzard as part of Battle.net service for any purpose.¹²³³

The defendants developed a server, known as the bnetd server, that was designed to emulate the Battle.net service so as to allow players to play their Blizzard games in an online multi-player mode through the bnetd server.¹²³⁴ In order to develop the bnetd server, the defendants had to reverse engineer the Blizzard games to learn the Battle.net protocol. In addition, because Blizzard games were designed to connect only to Battle.net servers, the defendants had to modify a computer file in the Blizzard games containing the Internet address of the Battle.net servers so as to cause the games to connect to a bnetd server instead. The defendants distributed a utility known as “BNS” that modified such file and caused Blizzard games to connect to the bnetd server rather than the Battle.net server. Once connected to the bnetd server through the modified Internet address file, a Blizzard game would send its CD Key to the bnetd server. When the bnetd server received the CD Key, unlike Battle.net, it did not determine whether the CD Key was valid or currently in use by another player. Instead, the bnetd server would always send the game an “okay” reply. Thus, both authorized as well as

¹²³¹ Id.

¹²³² Id. at 1169.

¹²³³ Id. at 1169-71.

¹²³⁴ Id. at 1172.

unauthorized or pirated copies of Blizzard games could be played in online mode through the bnetd server.¹²³⁵

The plaintiffs alleged two violations of the anti-circumvention provisions of the DMCA. First, they alleged that the defendants had violated Section 1201(a)(1)(A) in the course of development of the bnetd emulator by circumventing Blizzard's technological measures (the secret handshake) to gain access to Battle.net mode in the course of their reverse engineering.¹²³⁶ Although not clear from the court's opinion, the copyrighted work that the defendants gained access to via their circumvention was apparently the code in the Blizzard games that allowed them to operate in Battle.net mode and to communicate with the Battle.net service.

The defendants argued that their circumvention in the course of reverse engineering was permitted by Section 1201(f)(1) because it was done for the sole purpose of creating and distributing interoperable computer programs such as the bnetd server. They also argued that they had authority to access the Battle.net mode because they lawfully purchased the Blizzard software they reverse engineered.

The district court rejected these defenses. First, it ruled that it was "undisputed that defendants circumvented Blizzard's technological measure, the 'secret handshake,' between Blizzard games and Battle.net, that effectively control access to Battle.net mode."¹²³⁷ By its reference to "Battle.net mode," the court was again presumably referring to the code in the Blizzard games that allowed them to operate in Battle.net mode. The court rejected the defendants' reliance on Section 1201(f)(1), because the defendants had not developed an independently created computer program. The court noted that the defendants' actions in developing the bnetd server "extended into the realm of copyright infringement" because once game play started, "there are no differences between Battle.net and the bnetd emulator from the standpoint of a user who is actually playing the game."¹²³⁸ It is unclear from this language precisely what the basis was on which the court found copyright infringement. Perhaps the court believed that the defendants had copied code from the Battle.net server into the bnetd server, for earlier in the opinion the court noted that the plaintiffs contended "that the defendants not only copied code that would achieve interoperability, but also copied elements that would preserve player account information, display of icons, and presentation of ad

¹²³⁵ Id. at 1172-73.

¹²³⁶ Id. at 1183.

¹²³⁷ Id. at 1184-85.

¹²³⁸ Id. at 1185.

banners.”¹²³⁹ However, the opinion on appeal suggests that there was no copying of battle.net server code into the bnetd server.¹²⁴⁰

The court also rejected the Section 1201(f)(1) defense because it found that the defendants’ actions constituted more than enabling interoperability, since the emulator did not check the validity of the CD Key code passed from the game to the emulator, thereby allowing unauthorized copies of the Blizzard games to play on bnetd servers.¹²⁴¹

The plaintiffs also asserted that by distributing the bnetd software, the defendants had violated Section 1201(a)(2) by trafficking in devices whose only purpose was to circumvent their secret handshake and allow access to Battle.net mode. The defendants did not dispute the plaintiffs’ factual assertions, but instead asserted the defense of Sections 1201(f)(2)-(3) on the ground that those sections entitled them to distribute software to others for the purpose of enabling interoperability with the Blizzard games.¹²⁴² The court rejected the defenses on two grounds. First, the court ruled that the defendants’ purpose in distributing their software was not solely to enable interoperability, but rather to “avoid the restricted access to Battle.net.”¹²⁴³ In addition, the court reiterated its conclusion that the development and distribution of the bnetd software was infringing, and “persons who commit copyright infringement cannot benefit from the exemptions of § 1201(f).”¹²⁴⁴ Accordingly, the court granted the plaintiffs’ motion for summary judgment on their anti-circumvention and trafficking in anti-circumvention technology claims.¹²⁴⁵

On appeal, the Eight Circuit affirmed in an opinion that is even more terse and difficult to understand than the district court’s opinion. The court found a violation of Section 1201(a)(1) merely because unauthorized copies of Blizzard games were allowed to play through the bnetd server, even though the circumvention of the secret handshake did not cause the illegal copy of the Blizzard games to be made in the first place:

Blizzard games, through Battle.net, employed a technological measure, a software “secret handshake” (CD key), to control access to its copyrighted games. The bnetd.org emulator developed by Appellants allowed the Blizzard game to access Battle.net mode

¹²³⁹ Id. at 1184.

¹²⁴⁰ Davidson & Assocs. v. Jung, 422 F.3d 630, 636 (8th Cir. 2005) (“By necessity, Appellants used reverse engineering to learn Blizzard’s protocol language and to ensure that bnetd.org worked with Blizzard games. Combs used reverse engineering to develop the bnetd.org server, including a program called ‘tcpdump’ to log communications between Blizzard games and the Battle.net server.”).

¹²⁴¹ 334 F. Supp. 2d at 1185.

¹²⁴² Id. at 1185-86.

¹²⁴³ Id. at 1186.

¹²⁴⁴ Id. at 1187.

¹²⁴⁵ Id.

features without a valid or unique CD key. As a result, unauthorized copies of the Blizzard games were played on bnetd.org servers.¹²⁴⁶

The court also ruled that the anti-trafficking provisions of Section 1201(a)(2) had been violated because the bnetd.org emulator had as its sole purpose “to avoid the limitations of Battle.net.”¹²⁴⁷

With respect to the Section 1201(f) defense asserted by the defendants, the Eighth Circuit generalized all subsections of Section 1201(f) into one set of requirements as follows:

To successfully provide the interoperability defense under § 1201(f), Appellants must show: (1) they lawfully obtained the right to use a copy of a computer program; (2) the information gathered as a result of the reverse engineering was not previously readily available to the person engaging in the circumvention; (3) the sole purpose of the reverse engineering was to identify and analyze those elements of the program that were necessary to achieve interoperability of an independently created computer program with other programs; and (4) the alleged circumvention did not constitute infringement.¹²⁴⁸

In a very confusing portion of its opinion, the court then ruled that the exemption of Section 1201(f) was not available to the defendants because their circumvention constituted infringement. Precisely what that “infringement” was is unclear, although the court seems to base its holding on the fact that infringement by *third parties* was encouraged because pirated copies of Blizzard games could be played in multi-player mode through the bnetd server (even though the circumvention at issue did not cause or allow the pirated copies of the Blizzard games to be made in the first instance):

As detailed earlier, Blizzard’s secret handshake between Blizzard games and Battle.net effectively controlled access to Battle.net mode within its games. The purpose of the bnetd.org project was to provide matchmaking services for users of Blizzard games who

¹²⁴⁶ Davidson & Assocs. v. Jung, 422 F.3d 630, 640 (8th Cir. 2005). The Eighth Circuit distinguished the Lexmark decision by noting that in Lexmark, the Sixth Circuit had found Lexmark’s authentication sequence did not effectively control access to the Toner Loading Program and Printer Engine Program at issue, because it was not Lexmark’s authentication sequence that controlled access to such programs, but rather the purchase of a Lexmark printer that allowed access to the programs. “Here, Battle.net’s control measure was not freely available. Appellants could not have obtained a copy of Battle.net or made use of the literal elements of Battle.net mode without acts of reverse engineering, which allowed for a circumvention of Battle.net and Battle.net mode. Unlike in *Lexmark Int’l, Inc.*, Battle.net mode codes were not accessible by simply purchasing a Blizzard game or logging onto Battle.net, nor could data from the program be translated into readable source code after which copies were freely available without some type of circumvention.” Id. at 641. Although the preceding passage is confusing, it seems to imply (by the reference to “literal elements of Battle.net mode”) that the secret handshake controlled access to some Battle.net code within the Blizzard game itself. The Court’s reference to “Battle.net” seems to be referring to the Battle.net server software.

¹²⁴⁷ Id.

¹²⁴⁸ Id. at 641-42.

wanted to play in a multi-player environment without using Battle.net. The bnetd.org emulator enabled users of Blizzard games to access Battle.net mode features without a valid or unique CD key to enter Battle.net. The bnetd.org emulator did not determine whether the CD key was valid or currently in use by another player. As a result, unauthorized copies of the Blizzard games were freely played on bnetd.org servers. Appellants failed to establish a genuine issue of material fact as to the applicability of the interoperability exception.¹²⁴⁹

Based on these terse and confusing rulings, the court affirmed summary judgment in favor of the plaintiffs.¹²⁵⁰

(vi) Sony Computer Entertainment America v. Divineo

In Sony Computer Entertainment America, Inc. v. Divineo,¹²⁵¹ the court ruled that downstream lawful or fair uses of a circumvention device, including use to exercise Section 1201(f) rights, did not relieve the defendant from liability for trafficking in such devices under the DMCA. For a discussion of the details of the facts and rulings of the court, see Section II.G.1(b)(3) above.

(vii) Register of Copyrights' Report on Section 1201

In June 2017, the Copyright Office issued a report of the first comprehensive public study on the operation of Section 1201 since its enactment, titled "Section 1201 of Title 17: A Report of the Register of Copyrights."¹²⁵² In the report, the Copyright Office explores ambiguities with respect to whether the Section 1201(f) exemption for reverse engineering permits end users to circumvent for purposes of *enabling* interoperability among computer programs (e.g., using circumvention tools that Section 1201(f)(3) authorizes the creation and distribution of), or instead is limited to circumvention done solely for analytical purposes such as identification and analysis of elements necessary to achieve interoperability. Based on the statutory text, legislative history, and relevant case law, the Copyright Office concludes in the report that the stronger interpretation is that Section 1201(f) does permit circumvention to enable interoperability (i.e., circumvention for interoperation after reverse engineering has been performed) in certain circumstances, and subject to various statutory safeguards. The Copyright Office therefore concluded that amendment of Section 1201(f) was not currently necessary to allow consumers to engage in legitimate activity to enable interoperability.¹²⁵³

¹²⁴⁹ Id. at 642.

¹²⁵⁰ Id.

¹²⁵¹ 547 F. Supp. 2d 957 (N.D. Cal. 2006).

¹²⁵² The report may be found at <https://www.copyright.gov/policy/1201/section-1201-full-report.pdf>.

¹²⁵³ Id. at v, 63-71.

(viii) Authenticom v. CDK Global

In this complex antitrust litigation, one of the defendants, CDK Global, LLC, brought a counterclaim against the plaintiff Authenticom, Inc. under Section 1201(a)(2) based on Authenticom's alleged unauthorized access to CDK's enterprise software and computing platforms for automotive dealerships known as the Dealer Management System (DMS). According to CDK, Authenticom's business model revolved around improperly gaining free access to CDK's DMS, extracting and exporting the data from the DMS, often copying the data onto its own system, and then selling the data to third parties (principally vendors that provided software applications to support the dealers' operations). CDK alleged that Authenticom was able to do this by using login credentials, allegedly through unsecured means, acquired from dealers.¹²⁵⁴

Authenticom brought a motion to dismiss the Section 1201(a)(2) counterclaim on three grounds. First, Authenticom argued that CDK's claim failed because Authenticom was an authorized user. The court rejected this argument, ruling that CDK had sufficiently alleged a lack of authorization to survive a motion to dismiss. CDK alleged that Authenticom did not have CDK's permission or authorization to access or use CDK's DMS, that Authenticom was aware that CDK objected to its unauthorized access to the CDK DMS, and that Authenticom's contract with dealers made clear that it was not an agent of the dealers.¹²⁵⁵

Second, Authenticom argued that CDK had not plausibly alleged that it circumvented a technological measure, arguing that CDK's allegation that Authenticom obtained access to CDK's DMS by using dealer-provided login credentials did not establish circumvention under the DMCA. The court agreed that, if that is all CDK had alleged, such an allegation would be insufficient to establish circumvention. However, CDK also alleged that Authenticom implemented a software tool that automatically renewed user IDs that CDK had disabled, and DMS was not designed to allow third parties such as Authenticom to re-enable passwords that CDK intentionally disabled. Further, CDK alleged that Authenticom was able to modify its automated scripts in response to a CAPTCHA control designed by CDK to stop Authenticom's automated access. Authenticom argued that its "responding" to the CAPTCHA did not establish circumvention because passing a CAPTCHA did not involve descrambling, decrypting, or otherwise avoiding, bypassing, removing, deactivating, or impairing a technological measure. But the court noted that CDK had alleged that a CAPTCHA is a security measure intended to prevent and discourage the use of automated programs. Authenticom's use of an automated program to bypass CDK's use of a CAPTCHA therefore did avoid or bypass the technological measure taken by CDK to prevent the use of automated programs. The court therefore concluded that CDK plausibly had alleged circumvention under the DMCA.¹²⁵⁶

¹²⁵⁴ Authenticom, Inc. v. CDK Global, Inc. (In re Dealer Mgmt. Sys. Antitrust Litig.), 362 F. Supp. 3d 558, 563 (N.D. Ill. 2019).

¹²⁵⁵ Id. at 564, 567 & 570.

¹²⁵⁶ Id. at 571-72.

Third, Authenticom argued that CDK had not plausibly alleged that Authenticom's conduct fell outside of the reverse engineering provision of Section 1201(f)(2), which precludes liability for development and deployment of technological means to circumvent a technological measure for the purpose of enabling interoperability of an independently created computer program with other programs. CDK responded that Section 1201(f)(2) is a defense only to Section 1201(a)(2) and 1201(b)'s anti-trafficking provisions, not to Section 1201(a)(1)'s prohibition on unauthorized circumvention of technological measures. Authenticom did not respond to this argument by CDK and the court noted that it had thereby waived any argument in response. But regardless, the court noted that CDK alleged that Authenticom had done more than simply provide for interoperability between CDK's DMS and other software programs. Specifically, CDK alleged that Authenticom extracted data from CDK's DMS and improperly copied the data onto its own system. CDK therefore alleged that Authenticom did more than circumventing technological measures for the purpose of achieving interoperability. Accordingly, the court denied Authenticom's motion dismiss CDK's DMCA claim.¹²⁵⁷

(8) Encryption Research

Section 1201(g) provides that it is not a violation of the prohibition on circumventing a technological measure if such circumvention is done as an act of good faith "encryption research." "Encryption research" is defined as "activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products." "Encryption technology" is defined as "the scrambling and descrambling of information using mathematical formulas or algorithms." Sections 1201(g)(2)(C) and (D) require, however, that the person have made a good faith effort to obtain authorization before the circumvention, and that such acts not otherwise constitute a copyright infringement or violate other applicable law. Section 1201(g)(5) required that a report be generated to Congress on encryption technologies, with legislative recommendations (if any), not later than one year after enactment of the bill.

(9) Protection of Minors

Section 1201(h) provides that a court, in applying the prohibitions of Section 1201(a) against the manufacture or trafficking in a component or part designed to circumvent technological measures, may consider the necessity of such component or part for its intended and actual incorporation into a product whose sole purpose is to prevent the access of minors to material on the Internet.¹²⁵⁸

¹²⁵⁷ Id. at 572-73.

¹²⁵⁸ An earlier version of H.R. 2281 would have expanded this exception to also allow a parent to circumvent a technological measure controlling access to a test or evaluation of that parent's minor child's abilities by a nonprofit educational institution if the parent attempted to obtain authorization before the circumvention and the circumvention was necessary to obtain a copy of the test or evaluation.

(10) Protection of Personally Identifying Information

Section 1201(i) provides that it is not a violation of the Section 1201(a)(1)(A) prohibition on circumventing a technological measure if such measure, or the work it protects, is capable of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected, or if the measure in the normal course of its operation or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work, without providing conspicuous notice of such collection or dissemination to such person and the capability to prevent or restrict the same, and the circumvention is carried out solely to prevent such collection or dissemination. If a technological measure is disclosed to a user as not being capable of collecting or disseminating personally identifying information, then the exception of Section 1201(i) does not apply.

(11) Security Testing

Section 1201(j) provides that it is not a violation of the prohibitions of Sections 1201(a)(1)(A) and 1201(a)(2) if a person is engaged in “security testing,” which is defined to mean accessing a computer, computer system, or computer network solely for the purpose of good faith testing, investigating or correcting a security flaw or vulnerability with the authorization of the owner or operator, provided that such act does not otherwise constitute a violation of applicable law (including the Computer Fraud and Abuse Act of 1986).

(12) Copy Restrictions To Be Built Into VCRs and Camcorders

Section 1201(k) dictates that certain technological capabilities be built into consumer analog video cassette recorders (VCRs) and camcorders (professional analog video cassette recorders are exempted) to protect certain analog television programming and prerecorded movies. Specifically, effective 18 months after enactment of the DMCA, most formats of consumer analog¹²⁵⁹ VCRs and camcorders must contain one of two forms of copy control technology in wide use in the market today – either the “automatic gain control technology” (which causes distortion in the images upon playback) or the “colorstripe copy control technology” (which causes distracting visible color stripes to appear through portions of the viewable picture in normal viewing mode). Effective immediately, Section 1201(k) also prohibits tampering with these analog copy control technologies to render them ineffective. The Conference Report accompanying H.R. 2281¹²⁶⁰ states that Congress intended this Section to prohibit the manufacture and sale of “black box” devices and software “hacking” that defeat these copy control technologies.

¹²⁵⁹ Page 68 of the Conference Report states, “The conferees also acknowledge that numerous other activities are underway in the private sector to develop, test, and apply copy control technologies, particularly in the digital environment. Subject to the other requirements of this section, circumvention of these technologies may be prohibited under this Act.”

¹²⁶⁰ H.R. Rep. No. 105-796, at 78 (1998).

Section 1201(k) defines certain specific encoding rules that such devices must implement in order to preserve the capability to perform long-standing consumer home taping practices. Specifically, such devices cannot limit the copying of traditional broadcasts of programming through basic or extended basic tiers of programming services, although they may limit the copying of pay-per-view, near video-on-demand or video-on-demand transmission, or content stored on prerecorded media, as well the making of second generation copies where the original transmission was through a pay television service (such as HBO, Showtime or the like).

(13) Other Cases Filed Under the Anti-Circumvention Provisions

Several other anti-circumvention cases have been filed under the DMCA:

(i) Sony Computer Entertainment, Inc. v. Connectix, Inc.

On Jan. 27, 1999, Sony Computer Entertainment, Inc. and its U.S. subsidiary Sony Computer Entertainment America, manufacturers and distributors of the Sony PlayStation, filed suit against Connectix, Inc., a company that had developed a software emulator called the “Virtual Game Station” that would enable video games written for the PlayStation to run on Apple computers. In order to create the emulator, Connectix disassembled and reverse engineered the PlayStation’s operating system. The plaintiff’s complaint included claims for copyright infringement, trademark dilution, and circumvention of technological protection measures.¹²⁶¹

The circumvention claim was based on the fact that the PlayStation and its video games each contain embedded technological measures to prevent counterfeit games from running on the PlayStation, and the alleged fact that Connectix’s emulator software did not contain such technological measures, thus enabling counterfeit games to run on it. The plaintiffs contended that omission of the PlayStation’s technological measures constituted an unlawful circumvention of those measures. In its opposition to the plaintiffs’ motion for a temporary restraining order, Connectix asserted that its emulator did in fact implement the PlayStation’s technological measures and could not run counterfeit games. Thus, the alleged factual predicate on which the plaintiffs based their circumvention claim was apparently missing. On Feb. 4, 1999, the district court judge denied the plaintiffs’ motion for a temporary restraining order.¹²⁶²

Even if Connectix’s emulator software did not contain the technological measures of the PlayStation, the plaintiffs’ circumvention claim appears to be flawed for several reasons. First, the DMCA’s prohibition under Section 1201(a)(1) on circumvention of technological measures controlling access was not yet in effect at the time the complaint was filed, and the DMCA contains no prohibition on the act of circumventing copy controls. Second, Connectix’s emulator did not actively “circumvent” anything in the games it could run. At most, it simply allegedly

¹²⁶¹ See Band & Issihiki, supra note 1208, at 8.

¹²⁶² Id. at 8-9. On appeal, the Ninth Circuit ultimately held that Connectix’s reverse engineering of the Sony Playstation fell within the fair use doctrine. See Sony Computer Entertainment, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000). The Ninth Circuit’s opinion did not address the DMCA issues.

operated regardless of whether the video games contained the authentication signals required by the PlayStation (i.e., it allegedly ignored the authentication signal of the PlayStation). But Section 1201(c)(3) provides that Section 1201 does not require a computing product to “provide for a response to any particular technological measure,” so long as the product is not primarily designed or produced for the purpose of circumventing a technological measure or has only limited commercially significant purposes or uses other than the same. Because the Connectix emulator was not primarily designed to circumvent technological measures, but rather to run legitimate PlayStation games, it should probably fall within the savings clause of Section 1201(c)(3).¹²⁶³

(ii) RealNetworks, Inc. v. Streambox Inc.

On Dec. 20, 1999, RealNetworks, Inc., the developer and distributor of various versions of the “RealPlayer,” which embodied “streaming” technology that allowed Internet users to obtain real-time delivery and instant playback of audio and video content over the Internet, brought suit against Streambox, Inc.¹²⁶⁴ RealNetworks’ products embodied anti-piracy technology. Specifically, RealNetworks supplied copyright holders with a product known as “RealProducer,” which converted ordinary audio and video files into digitized “RealAudio” and “RealVideo” files. RealNetworks also offered a “RealServer” product to copyright holders that allowed them to distribute their copyrighted material in a secure format designed to interact only with RealPlayers to further prevent unauthorized access to copyrighted content.¹²⁶⁵

RealNetworks based its complaint on the following three products developed and distributed by Streambox:

“Streambox Ripper,” which converted any RealAudio file to a file in the format of Windows Media Audio (WMA), MPEG-Layer 3 (MP3), or Microsoft Windows Wave Format (WAV). Once in any of these three formats, an audio file could be copied, stored, or freely distributed, thereby circumventing RealNetworks’ security measures.¹²⁶⁶

“Streambox VCR,” which mimicked a RealPlayer, tricking RealServers into interacting with it and distributing both RealAudio and RealMedia files to it, thereby also circumventing the RealNetworks’ security measures.¹²⁶⁷

¹²⁶³ Band & Issihiki, *supra* note 1208, at 8-9.

¹²⁶⁴ Complaint for Violation of The Digital Millennium Copyright Act, Contributory, Vicarious and Direct Copyright Infringement, Tortious Interference with Contract, and Lanham Act Violations, RealNetworks, Inc. v. Streambox Inc., No. C99-2070Z (W.D. Wa. Dec. 20, 1999), available as of Dec. 30, 1999 at www.realnetworks.com/company/pressroom/pr/99/rnwk_complaint.html.

¹²⁶⁵ *Id.* ¶ 6.

¹²⁶⁶ *Id.* ¶¶ 12-13.

¹²⁶⁷ *Id.* ¶¶ 17-19.

“Streambox Ferret,” which was supposedly designed to work with and enhance the functionality of RealPlayers. RealNetworks alleged, however, that Streambox Ferret replaced the “snap.com” search engine on the RealPlayer’s search bar with a “Streambox” logo that diverted those using the RealPlayer’s search function from Snap’s search services (with whom RealNetworks had an exclusive arrangement) to a competing service operated by Streambox. In addition, RealNetworks alleged that Streambox Ferret corrupted completely the search functionality of the more recent versions of the RealPlayer.¹²⁶⁸

RealNetworks alleged, among other things, that (i) by circumventing RealNetworks’ technological measures that protect the rights of copyright owners to control whether an end-user can copy and distribute copyright owners’ works, both Streambox Ripper and Streambox VCR violated Section 1201(b) of the DMCA,¹²⁶⁹ and (ii) because the installation of Streambox Ferret modified the graphical user interface and computer code of RealPlayer, thereby creating an unauthorized derivative work, Streambox’s distribution of Streambox Ferret made it contributorily liable for copyright infringement, as well as vicariously liable, since Streambox allegedly controlled and profited from the infringement.¹²⁷⁰

In a decision issued Jan. 18, 2000, the court entered a preliminary injunction against Streambox, enjoining the manufacturing and distribution of Streambox VCR and Streambox Ferret, but not of Streambox Ripper.¹²⁷¹ This case raised three important procedural issues with respect to the DMCA. First, the case raised the interesting issue of who has standing to invoke the remedies of the DMCA – specifically, whether RealNetworks should be considered a proper party to bring the lawsuit, since the material that Streambox Ripper and Streambox VCR placed into a different file format (i.e., allegedly circumvented a protection measure for) was copyrighted, not by RealNetworks, but by its customers. As discussed further below, Section 1203 of the DMCA provides: “Any person injured by a violation of section 1201 or 1202 may bring a civil action in an appropriate United States district court for such violation.” Significantly, the reference to “any person” suggests that Section 1203 does not limit its scope to the copyright owner of the material with respect to which a technological protection measure has been circumvented, and the court so held. Specifically, the court ruled that RealNetworks had standing to pursue DMCA claims under Section 1203 based on the fact that it affords standing to “any person” allegedly injured by a violation of Section 1201 and 1202 of the DMCA.¹²⁷²

¹²⁶⁸ Id. ¶¶ 22-24.

¹²⁶⁹ Id. ¶¶ 33-35 & 41-43.

¹²⁷⁰ Id. ¶¶ 48-49.

¹²⁷¹ RealNetworks, Inc. v. Streambox Inc., 2000 U.S. Dist. LEXIS 1889 (W.D. Wa. 2000).

¹²⁷² Id. at *15-16. This holding is consistent with CSC Holdings, Inc. v. Greenleaf Electronics, Inc., 2000 U.S. Dist. LEXIS 7675 (N.D. Ill. 2000). In that case the plaintiff was a cable provider bringing suit against defendants under the DMCA for selling and distributing pirate cable descrambling equipment. The court held that the plaintiff was authorized to bring suit under Section 1203(a), as it was a person injured by a violation of the DMCA.

Second, the case raised the issue of what type of “injury” a plaintiff must show under Section 1203. Neither Section 1203 itself nor the legislative history illuminate this issue. In the instant case, RealNetworks was apparently relying on the argument that, because its customers were potentially injured by Streambox’s violation of Section 1201(b), RealNetworks itself was also injured. Although the court did not explicitly address this issue, by issuing a preliminary injunction, it implicitly accepted that RealNetworks was exposed to injury cognizable by the DMCA.

Third, the case raised the issue of whether a plaintiff who demonstrates a likelihood of success on the merits of claims under Section 1201 of the DMCA is entitled to a presumption of irreparable harm for purposes of a preliminary injunction, as would be the case in a showing of likely success on a claim for copyright infringement. The court noted that this must be considered an open issue: “Because the DMCA is a recently-enacted statute, there appears to be no authority holding that a plaintiff seeking a preliminary injunction who shows a reasonable likelihood of success on a claim arising under section 1201 of the DMCA is entitled to a presumption of irreparable harm.”¹²⁷³ Accordingly, the court considered in each instance whether Streambox’s violations of the DMCA were likely to cause irreparable harm.

Turning to the plaintiff’s claims under the anti-circumvention provisions of the DMCA, the court noted that RealNetworks’ products embodied two technological measures to control against unauthorized access or copying of content. First, a “Secret Handshake” – an authentication sequence that only RealServers and RealPlayers knew – ensured that files hosted on a RealServer could be sent only to a RealPlayer. Second, a “Copy Switch” was used, which was a piece of data in all RealMedia files that contained the content owner’s preference regarding whether or not the stream could be copied by end users.¹²⁷⁴ RealPlayers were designed to read the Copy Switch and obey the content owner’s wishes.

The court ruled that the Secret Handshake constituted a technological measure that effectively controlled access to copyrighted works within the meaning of Section 1201(a)(3)(B), and that the Copy Switch constituted a technological measure that effectively protected the right of a copyright owner to control the unauthorized copying of its work within the meaning of Section 1201(b)(2)(B). The court concluded that, because Streambox VCR was primarily designed to bypass the Secret Handshake and circumvent the Copy Switch (and had only limited commercially significant purposes beyond the same), Streambox VCR violated Sections 1201(a)(2) and 1201(b) of the DMCA.¹²⁷⁵

The court rejected Streambox’s defense that Streambox VCR allowed consumers to make “fair use” copies of RealMedia files under the Supreme Court’s decision in Sony Corp. v.

¹²⁷³ RealNetworks, 2000 U.S. Dist. LEXIS 1889 at *17.

¹²⁷⁴ Id. at *6.

¹²⁷⁵ Id. at *19-21.

Universal City Studios, Inc.¹²⁷⁶ The court distinguished the Sony case on the ground that, in Sony, the Supreme Court based its holding on the fact that video cassette recorders were mostly used by consumers for “time shift” viewing of programs, rather than the redistribution of perfect digital copies of audio and video files, and that substantial numbers of copyright holders who broadcast their works either had authorized or would not object to having their works time-shifted by private viewers. In the instant case, the court noted, copyright owners had specifically chosen to prevent the copying enabled by the Streambox VCR by putting their content on RealServers and leaving the Copy Switch off.¹²⁷⁷

In addition, the court, citing Nimmer’s copyright treatise, ruled that, by passage of the DMCA, Congress had decided that “those who manufacture equipment and products generally can no longer gauge their conduct as permitted or forbidden by reference to the *Sony* doctrine. For a given piece of machinery might qualify as a stable item of commerce, with a substantial noninfringing use, and hence be immune from attack under *Sony*’s construction of the Copyright Act – but nonetheless still be subject to suppression under Section 1201.”¹²⁷⁸ The court also rejected Streambox’s asserted defense under Section 1201(c)(3) of the DMCA, which it cited for the proposition that the Streambox VCR was not required to respond to the Copy Switch. The court noted that this argument failed to address Streambox VCR’s circumvention of the Secret Handshake, which was enough by itself to create liability under Section 1201(a)(2).¹²⁷⁹

Turning to the Streambox Ripper product, the court ruled that the plaintiff had not established a reasonable likelihood of success on its DMCA claim. RealNetworks maintained that the primary purpose and only commercially significant use for the Ripper was to enable consumers to prepare unauthorized derivative works of copyrighted audio or video content. The court rejected this argument, noting that the Ripper has legitimate and commercially significant uses to enable content owners, including copyright holders and those acquiring content with the content owner’s permission, to convert their content from the RealMedia format to other formats. Moreover, there was little evidence that content owners use the RealMedia format as a “technological measure” to prevent end users from making derivative works. In any case, the court found that RealNetworks had not introduced evidence that a substantial number of content owners would object to having end users convert RealMedia files that they legitimately obtained into other formats, or that Ripper would cause injury to RealNetworks.¹²⁸⁰

Finally, the court ruled that the plaintiff was entitled to a preliminary injunction with respect to Streambox Ferret. RealNetworks claimed that Streambox committed contributory or vicarious copyright infringement by distributing the Ferret to the public, because consumers who used the Ferret as a plug-in were making an unauthorized derivative work of the RealPlayer by

¹²⁷⁶ 464 U.S. 417 (1984).

¹²⁷⁷ RealNetworks, 2000 U.S. Dist. LEXIS at *21-22.

¹²⁷⁸ *Id.* at *23 (quoting 1 M. Nimmer & D. Nimmer, *Nimmer on Copyright* (1999 Supp.) § 12A.18[B]).

¹²⁷⁹ RealNetworks, 2000 U.S. Dist. LEXIS at *23.

¹²⁸⁰ *Id.* at *27-28.

changing the RealPlayer user interface to add a clickable button that permitted the user to access the Streambox search engine, rather than the Snap search engine. Although the court stated that it was not persuaded that RealNetworks had demonstrated that it was likely to succeed on its contributory/vicarious infringement claims on this basis, the court concluded that RealNetworks had raised serious questions going to the merits of its claims, and the balance of hardships clearly favored RealNetworks, because the addition of the alternative search engine afforded by the Ferret jeopardized RealNetworks' exclusive relationship with Snap.¹²⁸¹

In September of 2000, the parties settled the lawsuit pursuant to an agreement in which Streambox agreed to modify Streambox Ripper so that it no longer transformed RealMedia streams into other formats, to modify Streambox VCR so that it respected RealNetworks' copy protection features, to license RealNetworks' software development kit (which would allow Streambox to create versions of its products that worked with RealNetworks' copy protection technology), to stop distributing Streambox Ferret, and to pay an undisclosed sum of money.¹²⁸²

(iii) Universal City Studios, Inc. v. Reimerdes

In this case, the plaintiffs were copyright holders who distributed motion pictures encoded in a proprietary system for the encryption and decryption of data contained on digital versatile disks (DVDs) known as the Content Scramble System (CSS). The CSS technology was licensed to manufacturers of DVDs, who used it to encrypt the content of copyrighted motion pictures distributed in the DVD format. The plaintiffs filed suit under the DMCA against various defendants whom the plaintiffs alleged violated the anti-circumvention provisions of the DMCA by posting on their websites the source code of a program named "DeCSS," which was able to defeat DVD encryption using the CSS technology and enable viewing of DVD movies on unlicensed players and the making of digital copies of DVD movies.¹²⁸³ The plaintiffs sought a preliminary and permanent injunction to prevent the defendants from posting DeCSS on their Web site and from linking their site to others that posted DeCSS.¹²⁸⁴

On Jan. 20, 2000, the court entered a preliminary injunction against the defendants, restraining them from posting on any website or otherwise making available DeCSS or any other technology, product or service primarily designed or produced for the purpose of, or having only limited commercially significant purposes or use other than, circumventing CSS, or marketed by defendants or others acting in concert with them for use in circumventing CSS.¹²⁸⁵ In an opinion

¹²⁸¹ *Id.* at *30-33.

¹²⁸² "Early DMCA Lawsuit Settled, Streambox Will Modify Products to Prevent Digital Copying," *BNA's Electronic Commerce & Law Report* (Oct. 11, 2000) at 1019.

¹²⁸³ Universal City Studios Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

¹²⁸⁴ *Id.* at 303.

¹²⁸⁵ Preliminary Injunction, Universal City Studios, Inc. v. Reimerdes, No. 00 Civ. 0277 (LAK) (S.D.N.Y. Jan. 20, 2000) ¶ 2.

issued Feb. 2, 2000, the court set forth its findings of fact and conclusions of law supporting the preliminary injunction.¹²⁸⁶

On Aug. 17, 2000, after a bench trial, the court issued a permanent injunction against the defendants.¹²⁸⁷ The court ruled that DeCSS was clearly a means of circumventing CSS, a technological access control measure, that it was undisputed that DeCSS was designed primarily to circumvent CSS, and therefore that DeCSS constituted a prima facie violation of Section 1201(a)(2).¹²⁸⁸ The court rejected the defendants' argument that CSS did not "effectively control" access to the plaintiffs' copyrighted works because it was based on a 40-bit encryption key, which the defendants argued was a weak cipher. The court noted that Section 1201(a)(3)(B) provides that a technological measure "effectively controls access to a work" if it requires the application of information or a process with the authority of the copyright owner to gain access to a work. Because one cannot gain access to a CSS-protected work on a DVD without the application of three keys that are required by the player software and are made available only under license, CSS satisfied this definition. The court refused to import into the statute any requirement for a technologically "strong means" of protection.¹²⁸⁹

The court also rejected the defendants' argument that DeCSS was written to further the development of a DVD player that would run under the Linux operating system, as there allegedly were no Linux-compatible players on the market at the time. The court ruled that, even if there were so, it would be immaterial to whether the defendants had violated Section 1201(a)(2) by trafficking in DeCSS.¹²⁹⁰ "The offering or provision of the program is the prohibited conduct – and it is prohibited irrespective of why the program was written, except to whatever extent motive may be germane to determining whether [the defendants'] conduct falls within one of the statutory exceptions."¹²⁹¹

The court rejected a number of other defenses under the DMCA asserted by the defendants. First, for the reasons set forth in Section II.G.1(g) above in the discussion of Section 1201(f), the court rejected the defendants' argument that the reverse engineering exception of Section 1201(f) was applicable.

Second, the defendants asserted the encryption research defense under Section 1201(g), which requires a showing that the person asserting the defense lawfully obtained the encrypted

¹²⁸⁶ Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211 (S.D.N.Y. 2000).

¹²⁸⁷ Universal City Studios Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000). An amended final judgment was entered by the court on Aug. 23, 2001, enjoining the defendants from posting DeCSS on their web site and from knowingly linking their web site to any other web site on which DeCSS was posted. Universal City Studios Inc. v. Reimerdes, 111 F. Supp. 2d 346 (S.D.N.Y. 2000).

¹²⁸⁸ 111 F. Supp. 2d at 317-19.

¹²⁸⁹ Id. at 318. The court cited legislative history to the effect that a technological measure "effectively controls access" to a copyrighted work merely if its *function* is to control access. Id. at 317-18.

¹²⁹⁰ Id. at 319.

¹²⁹¹ Id.

copy of the work being studied, the circumvention act at issue is necessary to conduct encryption research, the person made a good faith effort to obtain authorization before the circumvention, and the act does not constitute copyright infringement. The court held that the defendants had failed to prove that any of them were engaged in good faith encryption research, nor was there any evidence that the defendants made any effort to provide the results of the DeCSS effort to the copyright owners (which Section 1201(g)(3) instructs the court to take into account in assessing whether one is engaged in good faith encryption research), nor any evidence that any of them made a good faith effort to obtain authorization from the copyright owners.¹²⁹²

Third, the defendants asserted the security testing defense under Section 1201(j). The court rejected this defense, which is limited to “assessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting [of a] security flaw or vulnerability, with the authorization of the owner or operator,” because the record did not establish that DeCSS has anything to do with testing computers, computer systems, or computer networks, and the defendants had not sought authorization for their activities.¹²⁹³

Fourth, the defendants claimed that they were engaged in a fair use under Section 107 of the copyright statute. The court categorically rejected this defense, noting that the defendants were not being sued for copyright infringement, but rather for offering to the public technology primarily designed to circumvent technological measures that control access to copyrighted works.¹²⁹⁴ The court held that fair use is not a defense to Section 1201(a)(2) of the DMCA: “If Congress had meant the fair use defense to apply to such actions, it would have said so. Indeed, as the legislative history demonstrates, the decision not to make fair use a defense to a claim under Section 1201(a) was quite deliberate.”¹²⁹⁵ The court noted that Congress had provided a vehicle, in the form of rulemaking by the Register of Copyrights, by which particular classes of copyrighted works could be exempted from the prohibitions if noninfringing uses of those classes of works would be affected adversely by Section 1201(a)(1).¹²⁹⁶ The court also rejected the defendants’ assertion that, because DeCSS could be used for noninfringing purposes, its distribution should be permitted under Sony Corp. v. Universal City Studios, Inc.¹²⁹⁷ The court elected to follow the holding in the RealNetworks case that a piece of technology might have a

¹²⁹² Id. at 320-21.

¹²⁹³ Id. at 321.

¹²⁹⁴ Id. at 322.

¹²⁹⁵ Id.

¹²⁹⁶ Id. at 323. The court, in a very lengthy analysis, also rejected various First Amendment challenges to the constitutionality of the anti-circumvention provisions of the DMCA. See id. at 325-341.

¹²⁹⁷ 464 U.S. 417 (1984).

substantial noninfringing use, and therefore be immune from attack under Sony, yet nonetheless be subject to suppression under Section 1201.¹²⁹⁸

Finally, in one of the most novel aspects of the opinion, the court addressed the issue whether the mere linking by the defendants to other Web sites on which DeCSS could be obtained should be deemed to be offering to the public or providing or otherwise trafficking in DeCSS within the prohibitions of Section 1201(a)(2). The court, noting that the dictionary definitions of the words “offer,” “provide,” and “traffic” are broad, ruled that “the anti-trafficking provision of the DMCA is implicated where one presents, holds out or makes a circumvention technology or device available, knowing its nature, for the purpose of allowing others to acquire it.”¹²⁹⁹ Accordingly, the court enjoined the defendants from providing three types of links:

Links “to sites that automatically commence the process of downloading DeCSS upon a user being transferred by defendants’ hyperlinks.” The court ruled that this was the functional equivalent of the defendants transferring the DeCSS code themselves.¹³⁰⁰

Links “to web pages that display nothing more than the DeCSS code or present the user only with the choice of commencing a download of DeCSS and no other content. The only distinction is that the entity extending to the user the option of downloading the program is the transferee site rather than defendants, a distinction without a difference.”¹³⁰¹

Links “to pages that offer a good deal of content other than DeCSS but that offer a hyperlink for downloading, or transferring to a page for downloading, DeCSS,” based on the given facts, in which the defendants had intentionally used and touted the links to “mirror” sites to help others find copies of DeCSS, after encouraging sites to post DeCSS and checking to ensure that the mirror sites in fact were posting DeCSS or something that looked like it, and proclaimed on their own site that DeCSS could be had by clicking on the links.¹³⁰²

¹²⁹⁸ Reimerdes, 111 F. Supp. 2d at 323. In the preliminary injunction proceeding, one of the defendants asserted a defense under Section 512(c) of the DMCA, discussed below, which limits liability of “service providers” for certain acts of infringement committed through systems or networks operated by them. The court rejected this defense on the ground that Section 512(c) provides protection only from liability for copyright infringement, and not for violations of the anti-circumvention provisions of Section 1201(a)(2). The court also ruled that the defendant had offered no proof that he was a “service provider” within the meaning of Section 512(c). 82 F. Supp. 2d at 217.

¹²⁹⁹ Reimerdes, 111 F. Supp. 2d at 325.

¹³⁰⁰ Id.

¹³⁰¹ Id.

¹³⁰² Id.

On appeal, the defendants renewed their attack on the constitutionality of the DMCA. In Universal City Studios Inc. v. Corley,¹³⁰³ the Second Circuit rejected such challenges and upheld the constitutionality of the DMCA anti-circumvention provisions. The court first rejected the defendants' argument that Section 1201(c)(1) should be read narrowly to avoid ambiguity that could give rise to constitutional infirmities. The defendants contended that Section 1201(c)(1) could and should be read to allow the circumvention of encryption technology when the protected material would be put to fair uses. The court disagreed that Section 1201(c)(1) permitted such a reading. "Instead, it clearly and simply clarifies that the DMCA targets the *circumvention* of digital walls guarding copyrighted material (and trafficking in circumvention tools), but does not concern itself with the *use* of those materials after circumvention has occurred."¹³⁰⁴ The court held that, in any event, the defendants did not claim to be making fair use of any copyrighted materials, and nothing in the injunction prohibited them from making such fair use.¹³⁰⁵ "Fair use has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user's preferred technique or in the format of the original."¹³⁰⁶

The court ruled that computer programs are not exempted from the category of First Amendment speech merely because their instructions require use of a computer. Rather, the ability to convey information renders the instructions of a computer program in source code form "speech" for purposes of the First Amendment.¹³⁰⁷ However, the court held that the "realities of what code is and what its normal functions are require a First Amendment analysis that treats code as combining nonspeech and speech elements, *i.e.*, functional and expressive elements."¹³⁰⁸ Accordingly, the scope of First Amendment protection for the DeCSS code at issue was limited.¹³⁰⁹

With this background, the court turned to a First Amendment analysis of the specific prohibitions of the injunction. With respect to the prohibition against posting of the DeCSS code, the court held that the prohibition was content neutral and was directed only toward the nonspeech component of DeCSS – "[t]he DMCA and the posting prohibition are applied to DeCSS solely because of its capacity to instruct a computer to decrypt CSS. That functional capability is not speech within the meaning of the First Amendment."¹³¹⁰ Therefore, the content-neutral posting prohibition, which had only an incidental effect on a speech component, would pass

¹³⁰³ 273 F.3d 429 (2d Cir. 2001).

¹³⁰⁴ Id. at 443 (emphasis in original).

¹³⁰⁵ Id. at 459.

¹³⁰⁶ Id.

¹³⁰⁷ Id. at 447.

¹³⁰⁸ Id. at 451.

¹³⁰⁹ Id. at 453.

¹³¹⁰ Id. at 454.

muster if it served a substantial governmental interest unrelated to the suppression of free expression, which the court found that it did.¹³¹¹

With respect to the prohibition against linking to other web sites posting DeCSS, the court again noted that a link has both a speech and a nonspeech component. “It conveys information, the Internet address of the linked web page, and has the functional capacity to bring the content of the linked web page to the user’s computer screen.”¹³¹² And again, the court ruled that the prohibition on linking was content neutral. “The linking prohibition applies whether or not the hyperlink contains any information, comprehensible to a human being, as to the Internet address of the web page being accessed. The linking prohibition is justified solely by the functional capability of the hyperlink.”¹³¹³ The court rejected the defendants’ argument that the prohibition burdened substantially more speech than necessary to further the government’s legitimate interest because it did not require an intent to cause harm by the linking, and that linking could be enjoined only under circumstances applicable to a print medium. The court found that the defendants’ arguments ignored the reality of the functional capacity of decryption computer code and hyperlinks to facilitate instantaneous unauthorized access to copyrighted materials by anyone anywhere in the world. Accordingly, “the fundamental choice between impairing some communication and tolerating decryption cannot be entirely avoided.”¹³¹⁴

Having rejected all constitutional challenges to the district court’s injunction, the Second Circuit affirmed the district court’s final judgment.¹³¹⁵ The defendants decided not to appeal the case further to the Supreme Court.¹³¹⁶

(iv) A Related DVD Case Involving Trade Secret Claims – DVD Copy Control Association, Inc. v. McLaughlin (the Bunner case)

This case,¹³¹⁷ although initially filed in state court alleging only misappropriation of trade secrets, presented another fact pattern amenable to a claim under the anti-circumvention provisions of the DMCA. The plaintiff in that case, DVD Copy Control Association, Inc. (DVD CCA),

¹³¹¹ *Id.* at 454-55. The court noted that it had considered the opinion of the California Court of Appeal in the *Bunner* case, discussed in subsection e. below and that to “the extent that *DVD Copy Control* disagrees with our First Amendment analysis, we decline to follow it.” *Id.* at 455 n.29. As noted in subsection e. below, the Supreme Court of California subsequently reversed the California Court of Appeal decision.

¹³¹² *Id.* at 456.

¹³¹³ *Id.*

¹³¹⁴ *Id.* at 458.

¹³¹⁵ *Id.*

¹³¹⁶ Lisa Bowman, “Copyright Fight Comes to an End” (July 3, 2002), available as of July 8, 2002 at <http://news.com.com/2102-1023-941685.html>.

¹³¹⁷ No. CV786804 (Santa Clara Superior Court, Dec. 27, 1999).

was the sole licensor of CSS.¹³¹⁸ The plaintiff alleged that various defendants had misappropriated trade secrets in CSS by posting on their websites proprietary information relating to how the CSS technology functions, the source code of DeCSS, and/or providing links to other websites containing CSS proprietary information and/or the DeCSS program.¹³¹⁹

On Dec. 29, 1999, the court denied an application by the plaintiff for a temporary restraining order that would have required the defendants to remove the DeCSS program and proprietary information from their websites, as well as links to other sites containing the same.¹³²⁰ However, on Jan. 21, 2000 (the day after the court in Reimerdes issued its preliminary injunction under the DMCA), the judge reversed course and issued a preliminary injunction prohibiting the defendants from “[p]osting or otherwise disclosing or distributing, on their websites or elsewhere, the DeCSS program, the master keys or algorithms of the Content Scrambling System (‘CSS’), or any other information derived from this proprietary information.”¹³²¹

In its order, the court stated that the evidence was fairly clear that the trade secret was obtained through reverse engineering, and acknowledged that reverse engineering is not considered “improper means” of obtaining a trade secret under the Uniform Trade Secrets Act. “The only way in which the reverse engineering could be considered ‘improper means’ herein would be if whoever did the reverse engineering was subject to the click license agreement which preconditioned installation of DVD software or hardware, and prohibited reverse engineering. Plaintiff’s case is problematic at this pre-discovery state. Clearly they have no direct evidence at this point that [defendant] Jon Johansen did the reverse engineering, and that he did so after clicking on any licence [sic] agreement.”¹³²² Nevertheless, without elaboration, the court found that the “circumstantial evidence, mostly due to the various defendants’ inclination to boast about their disrespect for the law, is quite compelling on both the issue of Mr. Johansen’s improper means [and] th[e] Defendants’ knowledge of impropriety.”¹³²³ The court found that the harm to the defendants of the injunction would be minimal, while without the injunction, “the Plaintiff’s right to protect this information as secret will surely be lost, given the current power of the Internet to disseminate information and the Defendants’ stated determination to do so.”¹³²⁴

¹³¹⁸ Id. ¶ 4.

¹³¹⁹ Id. ¶¶ 1, 27-29, 45-50, 60-61.

¹³²⁰ Deborah Kong, “DVD Movie Fight Loses,” *San Jose Mercury News* (Dec. 30, 1999) at 1C.

¹³²¹ Order Granting Preliminary Injunction, DVD Copy Control Assoc. v. McLaughlin (Sup. Ct., County of Santa Clara, Jan. 21, 2000), available as of Jan. 19, 2002 at www.eff.org/pub/Intellectual_property/Video/DVDCCA_case/20000120-pi-order.html.

¹³²² Id. at 2.

¹³²³ Id. at 2-3.

¹³²⁴ Id. at 3.

The court rejected the defendants' argument "that trade secret status should be deemed destroyed at this stage merely by the posting of the trade secret to the Internet. To hold otherwise would do nothing less than encourage misappropriators of trade secrets to post the fruits of their wrongdoing on the Internet as quickly as possible and as widely as possible, thereby destroying a trade secret forever. Such a holding would not be prudent in this age of the Internet."¹³²⁵ The court refused, however, to extend the injunction to links to other websites where DeCSS was posted. The court warned that a ban on Internet links would be "overbroad and burdensome," calling links "the mainstay of the Internet and indispensable to its convenient access to the vast world of information. A website owner cannot be held responsible for all of the content of the sites to which it provides links."¹³²⁶

In November 2001, a California Court of Appeal reversed the injunction on First Amendment grounds. In DVD Copy Control Assoc. v. Bunner,¹³²⁷ the court acknowledged that, if the trial court correctly concluded that the plaintiffs had established a reasonable probability of success, a preliminary injunction would be justified in the absence of any free speech concerns. Nevertheless, the court found that the preliminary injunction could not withstand First Amendment scrutiny. The court ruled that DeCSS was "speech" within the scope of the First Amendment because "[r]egardless of who authored the program, DeCSS is a written expression of the author's ideas and information about decryption of DVDs without CSS."¹³²⁸ The court then held that republication of DeCSS by defendant Bunner¹³²⁹ was "pure speech within the ambit of the First Amendment" and that the preliminary injunction therefore constituted an unlawful prior restraint.¹³³⁰ "[A] person who exposes the trade secret may be liable for damages if he or she was bound by a contractual obligation to safeguard the secret. And anyone who infringes a copyright held by [the plaintiff] or by an DVD content provider may be subject to an action under the Copyright Act. We hold only that a preliminary injunction cannot be used to restrict Bunner from disclosing DeCSS."¹³³¹

On appeal, the California Supreme Court reversed the California Court of Appeal's decision, ruling that the trial court's preliminary injunction did not violate the First Amendment.¹³³² Although the Court held that restrictions on the dissemination of computer code were subject to scrutiny under the First Amendment because the code was a means of

¹³²⁵ Id.

¹³²⁶ Id. at 4.

¹³²⁷ 60 U.S.P.Q.2d 1803 (Cal. Ct. App. 2001).

¹³²⁸ Id. at 1809.

¹³²⁹ According to Bunner, defendant Jon Johansen actually reverse engineered the CSS software and Bunner merely republished it. He argued that he had no reason to know that DeCSS had been created by improper use of any proprietary information since the reverse engineering of CSS performed by Johansen was not illegal under Norwegian law. Id. at 1805-06.

¹³³⁰ Id. at 1811.

¹³³¹ Id. at 1812.

¹³³² DVD Copy Control Ass'n v. Bunner, 31 Cal.4th 864 (2003).

expressing ideas,¹³³³ it found that the preliminary injunction passed scrutiny, assuming the trial court properly issued the injunction under California's trade secret law, because it was content neutral (and therefore not subject to strict scrutiny) and achieved the requisite balance of interests by burdening no more speech than necessary to serve the government interests at stake.¹³³⁴ The Court emphasized that its holding was "quite limited," and that its ruling that the preliminary injunction did not violate the free speech clauses of the United States and California Constitutions was based on the assumption that the trial court properly issued the injunction under California's trade secret law. "On remand, the Court of Appeal should determine the validity of this assumption."¹³³⁵

On remand, the California Court of Appeal held that the preliminary injunction was not warranted under California trade secret law because DeCSS had been so widely distributed on the Internet that it was no longer a trade secret.¹³³⁶ At the time of the hearing in the trial court for a preliminary injunction, the evidence showed that DeCSS had been displayed on or linked to at least 118 Web pages in 11 states and 11 countries throughout the world and that approximately 93 Web pages continued to publish information about DeCSS. Subsequent to the filing of the law suit, a campaign of civil disobedience began among the programming community to spread the DeCSS code as widely as possible. Persons distributed the code at the courthouse, portions of it appeared on tee shirts, and contests were held encouraging people to submit ideas about how to disseminate the information as widely as possible.¹³³⁷

The court stated, "Publication on the Internet does not necessarily destroy the secret if the publication is sufficiently obscure or transient or otherwise limited so that it does not become generally known to the relevant people, i.e., potential competitors or other persons to whom the information would have some economic value."¹³³⁸ However, in the instant case, the court held that the evidence in the case demonstrated that DeCSS had been published to "a worldwide audience of millions" and "the initial publication was quickly and widely republished to an eager audience so that DeCSS and the trade secrets it contained rapidly became available to anyone interested in obtaining them."¹³³⁹ Accordingly, the plaintiff had not established a likelihood of success on its trade secret claim because DeCSS had been so widely published that the CSS technology "may have lost its trade secret status."¹³⁴⁰

¹³³³ Id. at 876.

¹³³⁴ Id. at 877-85.

¹³³⁵ Id. at 889.

¹³³⁶ DVD Copy Control Ass'n Inc. v. Bunner, 116 Cal. App. 4th 241 (6th Dist. 2004).

¹³³⁷ Id. at 248-49.

¹³³⁸ Id. at 251.

¹³³⁹ Id. at 252-53.

¹³⁴⁰ Id. at 255.

In a related DeCSS case involving jurisdictional issues, defendant Matthew Pavlovich, a Texas resident who posted DeCSS on the web, was sued by the movie industry in California. A state judge granted an injunction against his posting of DeCSS on trade secret grounds. The California Supreme Court ruled that Pavlovich could not be sued in California because he did not have substantial ties to the state. In January of 2004, the U.S. Supreme Court reversed an emergency stay of the California Supreme Court's decision and lifted the injunction. Justice O'Connor noted in the order that there was no need to keep DeCSS a secret.¹³⁴¹

(v) A Related DVD Case – Norwegian Prosecution of Jon

Johansen

In January 2002, Norwegian prosecutors brought criminal charges against Jon Johansen, one of the original three authors of the DeCSS program, for violating Norwegian hacking laws.¹³⁴² On Jan. 11, 2002, the civil rights organization Electronic Frontier Norway (EFN) issued a press release calling for Johansen's acquittal and full redress.¹³⁴³ After a trial, a three-judge court in Oslo acquitted Johansen, ruling that consumers have rights to view legally obtained DVD films "even if the films are played in a different way than the makers had foreseen." On appeal, Johansen was again acquitted.¹³⁴⁴

(vi) Another Challenge to the DMCA – The Felten Case.

During 2000, the Secure Digital Music Initiative (SDMI) offered a cash prize to anyone who could break its watermark encryption scheme for the protection of digital content. A team of scientists, led by Prof. Edward Felten of Princeton University, was able to crack the scheme and desired to publish a paper on how they were able to do it. The RIAA threatened Prof. Felten, contending that publication of the paper would violate the anti-circumvention provisions of the DMCA. As a result of the threats, Prof. Felten withdrew publication of his paper from an April 2001 conference. In June 2001, he and seven other researchers, together with the Usenix Association (a professional organization that had accepted Felten's paper for a security symposium to be held during August 2001), filed a lawsuit against the RIAA, seeking a declaration that publication of their work would not violate the DMCA, and against the Justice Department to block it from prosecuting the symposium organizers for allowing the paper to be presented.¹³⁴⁵ On Nov. 28, 2001, a district judge in New Jersey dismissed the lawsuit, apparently concluding that neither the RIAA nor the Justice Department had imminent plans to seek to stop

¹³⁴¹ Samantha Chang, "Supreme Court Unscrambles DVD Decision" (Jan. 17, 2004), available as of Jan. 19, 2004 at www.reuters.com/newsArticle.jhtml?type=musicNews&storyID=4152687.

¹³⁴² Declan McCullagh, "Norway Cracks Down on DVD Hacker" (Jan. 10, 2002), available as of Jan. 19, 2002 at www.wired.com/news/politics/0,1283,49638,00.html.

¹³⁴³ The press release was available as of Jan. 19, 2002 at www.efn.no/freejon01-2002.html.

¹³⁴⁴ "Court Surprised DVD-Jon's Lawyer" (Dec. 22, 2003), available as of Dec. 22, 2003 at www.aftenposten.no/english/local/article.jhtml?articleID=696470.

¹³⁴⁵ Declan McCullagh, "Code-Breakers Go to Court" (June 6, 2001), available as of Jan. 19, 2002 at www.wired.com/news/mp3/0,1285,44344,00.html.

Prof. Felten from publishing his findings.¹³⁴⁶ Citing assurances from the government, the RIAA, and the findings of the district judge, in Feb. of 2002, Prof. Felten and his research team decided not to appeal the dismissal of their case.¹³⁴⁷

(vii) Pearl Investments, LLC v. Standard I/O, Inc.

In this case, Pearl hired Standard to perform software programming services to develop an automated stock-trading system (ATS). After completion of ATS, an employee of Standard named Chunn who had helped develop ATS, working on his own time, created software for his own experimental automated trading system, which he maintained on a server separate from the server that Pearl's ATS system was operating on, although Chunn's server was hosted by the same service provider as Pearl's ATS system.¹³⁴⁸ Pearl's ATS system operated on a virtual private network (VPN) that contained access restrictions implemented through a special router to the VPN.¹³⁴⁹ At one point, Pearl requested the service provider to install Linux on its ATS server. The service provider mistakenly installed Linux on Chunn's server, which was plugged into Pearl's router. Pearl alleged that a "tunnel" (a secure connection) was configured in the router that provided a connection between Chunn's server and Pearl's server, thereby allowing Chunn to circumvent Pearl's password-protected VPN and gain unauthorized access to its ATS system running on the VPN, which included Pearl's copyrighted software.¹³⁵⁰

Pearl brought claims against Standard and Chunn for, among other things, violation of Section 1201(a)(1)(A) of the DMCA based on the alleged creation of the tunnel. Both the plaintiff and the defendants sought summary judgment on the claim. The court ruled that Standard was entitled to summary judgment because the evidence was undisputed that Chunn, in developing and operating his automated trading system, was acting solely on his own and not as an employee of Standard. Standard could therefore not be held liable for his actions.¹³⁵¹

The court, however, denied summary judgment to Chunn. First, the court ruled that Pearl's VPN was the "electronic equivalent" of a locked door that fit the definition of a technological protection measure put in place by the copyright owner to control access to Pearl's copyrighted ATS software.¹³⁵² The court rejected the argument that the VPN did not effectively

¹³⁴⁶ Robert Lemos, "Court Dismisses Free-Speech Lawsuit" (Nov. 28, 2001), available as of Jan. 19, 2002 at <http://news.cnet.com/news/0-1005-200-8010671.html>.

¹³⁴⁷ Electronic Frontier Foundation press release, "Security Researchers Drop Scientific Censorship Case" (Feb. 6, 2002), available as of Feb. 10, 2002 at [www.eff.org/IP/DMCA/Felten v RIAA/20020206_eff_felten_pr.html](http://www.eff.org/IP/DMCA/Felten_v_RIAA/20020206_eff_felten_pr.html). The government stated in documents filed with the court in Nov. 2001 that "scientists attempting to study access control technologies" are not subject to the DMCA. *Id.*

¹³⁴⁸ *Pearl Investments, LLC v. Standard I/O, Inc.*, 257 F. Supp. 2d 326, 339-40 (D. Me. 2003).

¹³⁴⁹ *Id.* at 342, 349.

¹³⁵⁰ *Id.* at 341-42 & n.36, 349.

¹³⁵¹ *Id.* at 346-47, 349-50.

¹³⁵² *Id.* at 350.

control Chunn's access to the ATS system in view of the fact that he had written the ATS system himself and maintained a backup file of it for Pearl. "The question of whether a technological measure 'effectively controls access' is analyzed solely with reference to how that measure works 'in the ordinary course of its operation.' 17 U.S.C. § 1201(a)(3)(B). The fact that Chunn had alternative means of access to the works is irrelevant to whether the VPN effectively controlled access to them."¹³⁵³ Finally, the court ruled that because there was a factual dispute about whether only employees of the service provider, rather than Chunn, had configured the tunnel from Chunn's server to the Pearl VPN, or whether Chunn had configured his server and router to tunnel into Pearl's network, Chunn was not entitled to summary judgment on the DMCA claim.¹³⁵⁴

In a subsequent jury trial, the jury found for Chunn on Pearl's DMCA claim.¹³⁵⁵

(viii) 321 Studios v. Metro Goldwyn Mayer Studios, Inc.

In this case, 321 Studios marketed and sold software called DVD Copy Plus, which was capable of copying the video contents of a DVD, both encrypted and unencrypted with the DeCSS encryption scheme, onto a recordable CD. 321 Studios sought a ruling that its software did not violate the anti-circumvention provisions of the DMCA.¹³⁵⁶ The court ruled that the software's capability to decrypt DVDs encoded with CSS did violate the anti-circumvention provisions. The court first rejected 321 Studios' argument that CSS was not an effective technological measure because the CSS access keys were widely available on the Internet. The court held that "this is equivalent to a claim that, since it is easy to find skeleton keys on the black market, a deadbolt is not an effective lock to a door."¹³⁵⁷

With respect to the specific prohibition of Section 1201(a)(2), 321 Studios argued that it had the authority of the copyright holder to decrypt DVDs protected by CSS because its product worked only on original DVDs, and the purchaser of a DVD has the authority of the copyright holder to bypass CSS to play the DVD. The court rejected this argument, citing Universal City Studios, Inc. v. Corley¹³⁵⁸ for the proposition that purchase of a DVD does not authorize the purchaser to decrypt CSS, but rather only to view the content on the DVD. Only a licensed DVD

¹³⁵³ Id.

¹³⁵⁴ Id.

¹³⁵⁵ See Pearl Investments v. Standard I/O, Inc., 324 F. Supp. 2d 43 (2004) (rejecting Pearl's claim that the jury's verdict in favor of Chunn on the DMCA claim was inconsistent with its conclusion that Chunn's physical hookup to the Pearl system caused damage to Pearl).

¹³⁵⁶ 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1089-90 (N.D. Cal. 2004).

¹³⁵⁷ Id. at 1095.

¹³⁵⁸ 273 F.3d 429 (2d Cir. 2001).

player has the authority of the copyright holder to decrypt CSS and 321 Studios did not hold a CSS license.¹³⁵⁹

With respect to the specific prohibition of Section 1201(b)(1), 321 Studios argued that CSS was not a copy control measure because it controlled only access to content and did not control or prevent copying of DVDs. The court rejected this argument, noting that while it was technically correct that CSS controlled access to DVDs, “the purpose of this access control is to control copying of those DVDs, since encrypted DVDs cannot be copied unless they are accessed.”¹³⁶⁰ The court also rejected 321 Studios’ argument that the primary purpose of DVD Copy Plus was not to violate rights of a copyright holder since the software could be used for many purposes that did not involve accessing CSS or that involved making copies of material in the public domain or under fair use principles. In a potentially very broad holding, the court held that the downstream uses of DVD Copy Plus, whether legal or illegal, were irrelevant to determining whether 321 Studios itself was violating the DMCA.¹³⁶¹ “It is the technology itself at issue, not the uses to which the copyrighted material may be put. This Court finds, as did both the Corley and Elcom courts, that legal downstream use of the copyrighted material by customers is not a defense to the software manufacturer’s violation of the provisions of § 1201(b)(1).”¹³⁶²

321 Studios also argued that its software did not violate Section 1201(b)(2) because it used authorized keys to decrypt CSS. The court ruled that, “while 321’s software does use the authorized key to access the DVD, it does not have authority to use this key, as licensed DVD players do, and it therefore avoids and bypasses CSS.”¹³⁶³

Finally, 321 Studios argued that, under the common requirement of both Sections 1201(a)(2) and 1201(b)(1), its DVD Copy Plus software was not primarily designed and produced to circumvent CSS, but rather was designed and produced to allow users to make copies of all or part of a DVD, and that the ability to unlock CSS was just one of the features of its software. The court rejected this argument, noting that Sections 1201(a)(2) and 1201(b)(1) both prohibit any technology or product “or part thereof” that is primarily designed or produced for circumvention. Because it was undisputed that a portion of 321 Studios’ software was solely for the purpose of circumventing CSS, that portion of the software violated the DMCA.¹³⁶⁴

¹³⁵⁹ 321 Studios, 307 F. Supp. 2d at 1096.

¹³⁶⁰ Id. at 1097.

¹³⁶¹ Id.

¹³⁶² Id. at 1097-98.

¹³⁶³ Id. at 1098. This holding is contrary to that reached by the court in I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc., 307 F. Supp. 2d 521 (S.D.N.Y. 2004), discussed in the next subsection.

¹³⁶⁴ 321 Studios, 307 F. Supp. 2d at 1098. The court ruled that it could not determine on summary judgment whether the software had only limited commercially significant purposes other than circumvention, and that would be an issue a jury would have to decide. Id. The court also rejected 321 Studios’ challenge to the constitutionality of the anti-circumvention provisions on the ground that is unconstitutionally restricted 321

Accordingly, the court enjoined 321 Studios from manufacturing, distributing, or otherwise trafficking in any type of DVD circumvention software.¹³⁶⁵

(ix) Paramount Pictures Corp. v. 321 Studios.

The court in this case, in a very short opinion citing the Corley and Reimerdes cases and for the reasons stated therein, held that 321 Studios violated the anti-circumvention provisions of the DMCA by manufacturing and selling its software product that permitted the possessor of a DVD encoded with CSS to decode CSS and thereby make identical copies of the DVD. The court enjoined 321 Studios from manufacturing, distributing, linking to, or otherwise trafficking in any of its software products that were capable of decrypting CSS.¹³⁶⁶

(x) Macrovision Corp. v. 321 Studios

In this case, the same judge as in the Paramount Pictures case, in a one paragraph opinion that simply cited his earlier decision in the Paramount Pictures case, issued a preliminary injunction against 321 Studios barring it from selling the various versions of its DVD copying software.¹³⁶⁷ In August of 2004, 321 Studios reached a settlement with the motion picture industry, which included a financial payment and an agreement to stop distributing its DVD copying software worldwide, and ceased operations.¹³⁶⁸

(xi) Comcast of Illinois X v. Hightech Electronics, Inc.

In this case, the defendant Hightech set up a website named 1-satellite-dish.com that contained links to over thirty other websites selling illegal cable pirating devices. Comcast brought claims under Sections 1201(a)(2) and (b)(1) against the website as well as against Net Results, the named domain server for the 1-satellite-dish.com website.¹³⁶⁹ The defendants argued that only copyright holders can bring suit under the anti-circumvention provisions and that Comcast, in regard to the cable signals at issue, was not the copyright owner. The court rejected this argument, citing CSC Holdings, Inc. v. Greenleaf Electronics, Inc., 2000 U.S. Dist. LEXIS 7675 (N.D. Ill. 2000), which held that the plaintiff cable provider had standing to bring suit under Section 1203(a) against the defendants for selling and distributing pirate cable

Studios' right to tell others how to make fair use of a copyrighted work, impermissibly burdened the fair use rights of others, and exceeded the scope of Congressional powers. Id. at 1098-1105.

¹³⁶⁵ Id. at 1105.

¹³⁶⁶ Paramount Pictures Corp. v. 321 Studios, 69 U.S.P.Q.2d 2023, 2023-24 (S.D.N.Y. 2004).

¹³⁶⁷ Macrovision Corp. v. 321 Studios, 2004 U.S. Dist. LEXIS 8345 (S.D.N.Y. May 12, 2004).

¹³⁶⁸ "Maker of DVD-Copying Products Reaches Settlement Over Suits" (Aug. 10, 2004), available as of Aug. 11, 2004 at www.siliconvalley.com/mld/siliconvalley/news/editorial/9364923.htm.

¹³⁶⁹ Comcast of Illinois X v. Hightech Electronics, Inc., 2004 Copyr. L. Dec. ¶ 28,840 at pp. 37,299 & 37,232-33 (N.D. Ill. 2004).

descrambling equipment, as it was a person injured by a violation of the DMCA. Accordingly, the Comcast court concluded that Comcast could bring its claim under the DMCA.¹³⁷⁰

With respect to the merits of the DMCA claims, the court ruled that Comcast controlled through technological measures access to copyrighted programs it provided to its subscribers by scrambling those programs, and that such measures also protected the rights of the copyright owners in those programs, as required by Sections 1201(a)(2) and (b)(1). Citing the Reimerdes case, the court noted that there can be a violation of the DMCA for maintaining links to other websites that contain access to or information regarding circumvention technology. The court noted that the Intellectual Reserve case had refused to find contributory liability for posting links to infringing websites because there was no direct relationship between the defendant and the people who operated the websites containing the infringing material, and the defendants did not receive any kind of compensation from the linked websites.¹³⁷¹

By contrast, in the instant case, the court noted that Comcast had alleged that Hightech received compensation from the website operators that linked to 1-satellite-dish.com. In addition, the court found that Net Results, as the domain server of websites selling illegal cable equipment, could possibly be engaging in trafficking under the DMCA because it was allegedly assisting sellers of illegal cable equipment in distributing such equipment. The court therefore concluded that Comcast had sufficiently stated a claim against the defendants under the DMCA in trafficking or acting in concert with a person who had manufactured or distributed illicit circumvention equipment, and denied the defendants' motion to dismiss the DMCA claims.¹³⁷²

(xii) Davidson & Assocs. v. Internet Gateway

For a discussion of this case, which found violations of both the anti-circumvention and trafficking prohibitions of Section 1201, see Section II.G.1(g)(5) above.

(xiii) Agfa Monotype Corp. v. Adobe Sys.

This case addressed the issue of whether a passive bit or flag indicating the copyright owner's preference with respect to copying or distribution constitutes an effective technological access control measure or measure protecting copyright rights, and held that it does not. The plaintiffs were the copyright owners in about 3,300 copyrighted TrueType fonts. The plaintiffs alleged that Version 5 of Adobe's Acrobat product violated the anti-circumvention provisions of the DMCA because it ignored the "embedding bits" in certain of the plaintiffs' fonts that indicated whether the fonts were licensed for editing.¹³⁷³

¹³⁷⁰ Id. at 37,233.

¹³⁷¹ Id.

¹³⁷² Id. at 37,233-34.

¹³⁷³ Agfa Monotype Corp. v. Adobe Sys., 404 F. Supp. 2d 1030, 1031-32 (N.D. Ill. 2005).

Adobe Acrobat 5.0 was capable of embedding fonts into portable electronic documents stored in Adobe's Portable Document Format (PDF). The court described the technology of font embedding as follows:

A font is copied when it is embedded. Fonts are embedded through embedding bits. Embedding bits indicate to other programs capable of reading them, such as Adobe Acrobat, the font embedding licensing rights that the font vendor granted with respect to the particular font. The software application decides whether or not to embed the font based upon the embedding bit. An embedding bit cannot be read by a computer program until that program has already accessed the font data file. TrueType Fonts are not encrypted, scrambled, or authenticated. A TrueType Font data file can be accessed regardless of the font's embedding permissions. A program seeking to access a TrueType font need not submit a password or complete an authorization sequence to access, use or copy TrueType Fonts.¹³⁷⁴

The Microsoft TrueType Font specification defined four levels of embedding bit restrictions: Restricted (font cannot be embedded); Print & Preview (font can be embedded but the document must be opened as read-only and no edits may be applied to the document), Editable (font can be embedded and the document may be opened for reading and editing), and Installable.¹³⁷⁵ Acrobat 5.0 made it possible for the first time to embed in the "form field" or "free text annotation" of a PDF document¹³⁷⁶ any TrueType Font whose embedding bit was not set to "Restricted," including fonts whose embedding bit was set to "Print and Preview." This capability of Acrobat 5.0 was referred to as the "Any Font Feature."¹³⁷⁷

The plaintiffs contended that the Any Font Feature resulted in "editable embedding," because a recipient of a PDF file with embedded fonts could use the fonts to change the contents of a form field or free text annotation. The plaintiffs further contended that such editable embedding was possible only because Acrobat 5.0 allowed the embedding bits set by the plaintiffs to be "circumvented" in violation of the DMCA.¹³⁷⁸

The court rejected the plaintiffs' claims under both Sections 1201(a)(2) and 1201(b)(1) of the DMCA. With respect to Section 1201(a)(2), the court ruled that the plaintiffs' embedding bits did not effectively control access to the TrueType fonts. The court found that an embedding bit was a passive entity that did nothing by itself. Embedding bits were not encrypted, scrambled or authenticated, and software applications such as Acrobat 5.0 did not need to enter

¹³⁷⁴ Id. at 1031.

¹³⁷⁵ Id. at 1031-32.

¹³⁷⁶ A PDF form field was designed to allow a recipient to complete an electronic form and electronically return the information inputted on the form to the creator. A PDF free text annotation was designed to allow recipient to insert comments into the PDF document that could be viewed by the creator when electronically returned. Id. at 1033.

¹³⁷⁷ Id. at 1032.

¹³⁷⁸ Id. at 1034.

a password or authorization sequence to obtain access to the embedding bits or the specification for the TrueType font (which was publicly available for free download from the Internet). The embedding bits therefore did not, in their ordinary course of operation, require the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the plaintiffs' TrueType fonts, as required by Section 1201(a)(3)(B) in order for a technological measure to effectively protect access to a copyrighted work.¹³⁷⁹

In addition, the court ruled that Acrobat 5.0 did not contain technology, components or parts that were *primarily* designed to circumvent TrueType embedding bits. The court found that Acrobat 5.0 had many commercially significant purposes other than to circumvent embedding bits, even if it did circumvent them. The purpose of the embedded font capability in Acrobat 5.0 was so that electronic documents could look exactly the same when printed and viewed by a recipient as sent by the creator. The primary purpose of the forms feature was to allow recipients to complete electronic forms they receive and electronically return the information inputted on the form to the creator. Similarly, the commercial purpose of the free text annotation feature was to allow recipients to insert comments into the PDF that could be viewed by the creator when electronically returned. Nor was Acrobat 5.0 marketed for the primary purpose of circumventing the embedding bits – Adobe had made no mention of embedding bits, circumvention of embedding bits, or the Any Font Feature in any of its marketing materials for Acrobat 5.0.¹³⁸⁰

With respect to the plaintiffs' Section 1201(b)(1) claim, Adobe argued, and the court agreed, that the embedding bits did not constitute a technological measure that prevented, restricted, or otherwise limited the exercise of a right of copyright. The plaintiffs had already authorized the copy and distribution of their TrueType fonts for embedding in PDF documents for "Print and Preview" purposes. Acrobat 5.0 did not make an additional copy or distribution of a font to embed the font in free text annotations or form fields, and the plaintiffs' copyright did not give them the right to control subsequent use of lawfully made copies of the fonts.¹³⁸¹

In addition, for the same reasons noted in connection with the plaintiffs' Section 1201(a)(2) claim, the court ruled that Acrobat 5.0 as a whole and the parts thereof were not primarily designed or promoted for font embedding purposes and had many other commercially significant purposes other than circumventing the embedding bits associates with the plaintiffs' TrueType fonts. Accordingly, the court granted Adobe's motion for summary judgment with respect to the plaintiffs' anti-circumvention claims.¹³⁸²

¹³⁷⁹ *Id.* at 1036-37.

¹³⁸⁰ *Id.* at 1032-33.

¹³⁸¹ *Id.* at 1038-40.

¹³⁸² *Id.* at 1040.

(xiv) Macrovision v. Sima Products Corp.

In Macrovision v. Sima Products Corp.,¹³⁸³ the court held that the defendant's products, which eliminated Macrovision's Analog Copy Protection (ACP) signals imprinted on DVDs containing copyrighted works to prevent the copying of the DVDs, violated the anti-circumvention provisions. The ACP system inserted additional information in the non-visible portion of the analog signal, the practical effect of which was to render videotaped copies of the analog signal so visually degraded as to be unwatchable. The defendant's devices eliminated Macrovision's ACP from an analog signal. The removal function was effectuated by a single chip, usually the SA7114 chip from Philips. Macrovision contended, and Sima did not dispute, that Sima's devices could be fitted with an alternate chip manufactured by Philips that, under license from Macrovision, would recognize the ACP and not allow for its circumvention.¹³⁸⁴

Sima contended that its devices were intended primarily to allow the consumer to make "fair use" backup copies of a DVD collection. The court noted, however, that although the DMCA provides for a limited "fair use" exception for certain *users* of copyrighted works under Section 1201 (a)(2)(B), the exception does not apply to *manufacturers* or *traffickers* of the devices prohibited by Section 1201(a)(2).¹³⁸⁵

Sima argued that the "primary purpose" of its devices was not circumvention. The court rejected this argument, noting that, although some of the devices had some auxiliary functions, Sima did not argue that it was necessary for the device to be able to circumvent ACP in order to perform those functions. Nor did Sima argue that using the Macrovision-licensed Philips chips would prevent the devices from performing the auxiliary functions or facilitating the copying of non-protected works, such as home videos. Accordingly, the devices had only limited commercially significant purposes or uses other than circumvention.¹³⁸⁶ The court also noted that Sima had touted on its web site the devices' capability of circumventing copy protection on copyrighted works. And the DMCA does not provide an exception to the anti-circumvention provisions for manufacturers of devices designed to enable the exercise of fair use rights. Finally, the court noted that in any event Sima had cited no authority, and the court was aware of none, for the proposition that fair use includes the making of a backup copy.¹³⁸⁷ Accordingly, the court preliminarily enjoined Sima from selling its devices and any other products that circumvented Macrovision's copyright protection technologies in violation of the DMCA.¹³⁸⁸

¹³⁸³ 2006 U.S. Dist. LEXIS 22106 (S.D.N.Y. Apr. 20, 2006).

¹³⁸⁴ Id. at *2-3.

¹³⁸⁵ Id. at *2-3, *6.

¹³⁸⁶ Id. at *6-7.

¹³⁸⁷ Id. at *7-8.

¹³⁸⁸ Id. at *11-12.

(xv) Nordstrom Consulting, Inc. v. M&S Technologies, Inc.

In Nordstrom Consulting, Inc. v. M&S Technologies, Inc.,¹³⁸⁹ Nordstrom, acting as a consultant, developed software for a visual eye chart to be distributed as part of M&S's visual acuity systems. Nordstrom retained ownership of the copyrights in the software and, after a falling out with M&S, assigned the copyrights to a separate corporation. After leaving M&S, the plaintiffs alleged that M&S violated the DMCA by circumventing the password protection on a computer used by Nordstrom in order to gain access to the software.¹³⁹⁰ The court rejected this claim. Citing the Chamberlin v. Skylink case, the court noted that there must be a showing that the access resulting from the circumvention led to infringement, or the facilitation of infringement, of a copyrighted work, and the plaintiffs had failed to make such a showing. The court noted it was undisputed that the defendant had accessed the software in order to repair or replace the software of a client of M&S and a valid licensee of the software, so the circumvention of the password did not result in an infringement or the facilitation of infringement.¹³⁹¹

M&S, in turn, alleged that Nordstrom had violated the DMCA by circumventing the digital security of M&S's computer network. M&S's network was divided into two parts, one dealing with visual acuity systems and one with hotel/hospitality businesses. M&S asserted that, while Nordstrom had a password to access the acuity side of the system, he did not have a password to access the hotel side, yet Nordstrom claimed to have accessed the hotel side. The court denied summary judgment on M&S's claim because of factual disputes. Nordstrom asserted that he did not access the hotel side of the system and that any materials on the hotel side were not registered copyrights. By contrast, M&S had offered evidence that Nordstrom accessed the hotel side of the system, and alleged that the hotel side contained copyrighted works.¹³⁹²

(xvi) Dice Corp. v. Bold Technologies

Both the plaintiff and the defendant provided software for companies in the alarm industry. The defendant wrote an extraction program to extract customer data from the plaintiff's software (written in Thoroughbred basic) and convert it into a format that could be read by the defendant's software (written in C++ and Visual Basic). The database files where the customer data was stored by the plaintiff's software were not subject to any access or security features and could be accessed by anyone who had a copy of Thoroughbred basic. No administrative password was required to run queries on the database.¹³⁹³

¹³⁸⁹ 2008 U.S. Dist. LEXIS 17259 (N.D. Ill. Mar. 4, 2008).

¹³⁹⁰ Id. at *3-8.

¹³⁹¹ Id. at *23-24.

¹³⁹² Id. at *30-31.

¹³⁹³ Dice Corp. v. Bold Technologies, 913 F. Supp. 2d 389, 392, 395-96 & 400 (E.D. Mich. 2012).

The plaintiff's complaint alleged that encryption of its software constituted a technological measure that effectively controlled access to its products and that the defendant's use of former employees of the plaintiff with knowledge of methods to circumvent such encryption permitted the defendant to access the plaintiff's software without permission, in violation of the anti-circumvention provisions of the DMCA. The court granted the defendant summary judgment on this claim, finding that the plaintiff had produced no evidence that the defendant accessed any source code (which one of the plaintiff's employees admitted during discovery was not in fact encrypted) or other copyrighted material of the plaintiff. Rather, the defendant had accessed through its extraction program only customer data that was owned by the user of the plaintiff's software, which data was neither encrypted nor protected against access by any password or other technological measure.¹³⁹⁴

(14) Criminal Prosecutions Under the DMCA

(i) The Sklyarov/Elcomsoft Case

Dmitry Sklyarov, a 27-year-old Russian programmer who worked for a Russian company called Elcomsoft, helped create the Advanced eBook Processor (AEBPR) software, which enabled eBook owners to translate from Adobe's secure eBook format into the more common Portable Document Format (PDF). The software worked only on legitimately purchased eBooks. Sklyarov was arrested at the behest of Adobe Systems, Inc. on July 17, 2001 in Las Vegas after he delivered a lecture at a technical convention, and charged by the Dept. of Justice with criminal violations of the DMCA for distributing a product designed to circumvent copyright protection measures. He was subsequently released on \$50,000 bail and restricted to California.¹³⁹⁵

On Dec. 13, 2001, the U.S. government permitted Sklyarov to return home to Russia with his family, essentially dropping prosecution of him in return for his agreement to testify against his employer Elcomsoft in criminal proceedings the government brought against Elcomsoft. In early Feb. 2002, the Electronic Frontier Foundation, joined by The Computing Law and Technology and U.S. Public Policy Committees of the Association for Computing Machinery, the American Association of Law Libraries, the Electronic Privacy Information Center, the Consumer Project on Technology, Computer Professionals for Social Responsibility, and the Music Library Association, filed an amicus brief, along with a brief from 35 law professors, supporting a motion by Elcomsoft to dismiss the case. Elcomsoft's motion and the Electronic Frontier Foundation's brief argued that the DMCA should be found unconstitutional because it impinges on protected speech and stifles technological innovation.

Elcomsoft's motion to dismiss and its challenge on constitutional grounds were rejected by the court in an opinion issued on May 8, 2002.¹³⁹⁶ The court concluded that Congress intended to ban all circumvention tools and rejected Elcomsoft's argument that Congress

¹³⁹⁴ *Id.* at 409-11.

¹³⁹⁵ This information is taken from the Free Dmitry Sklyarov! web site at www.freesklyarov.org.

¹³⁹⁶ United States v. Elcom Ltd., 62 U.S.P.Q.2d 1736 (N.D. Cal. 2002).

intended to ban only those circumvention devices that would facilitate copyright infringement.¹³⁹⁷ The court also specifically concluded that “[n]othing within the express language [of the anti-circumvention provisions] would permit trafficking in devices designed to bypass use restrictions in order to enable a fair use, as opposed to an infringing use. Instead, all tools that enable circumvention of use restrictions are banned, not merely those use restrictions that prohibit infringement.”¹³⁹⁸ The court rejected the constitutional challenges on a rationale very similar to that of the Second Circuit’s opinion in the Corley case,¹³⁹⁹ discussed in Section II.G.1(m)(4) above. On Dec. 17, 2002, after a two week trial, a jury acquitted Elcomsoft of criminal charges under the DMCA. The jury foreman told the press that some jurors were concerned about the scope of the DMCA and whether it curtailed the fair use of material simply because it was in electronic format. “Under the eBook formats, you have no rights at all, and the jury had trouble with that concept,” the foreman reported.¹⁴⁰⁰

(ii) Other Criminal Prosecutions Under the DMCA

In Feb. of 2003, the operator of a web site, iSoNews.com, pleaded guilty to criminal DMCA violations for sale of “mod” chips that allowed Microsoft Xbox and Sony Playstation owners to modify their devices so they could use them to play illegally copied games. As part of a plea bargain, the defendant turned over the site’s domain name to the control of the U.S. Department of Justice, which then put a notice on the site stating that it had been surrendered to U.S. law enforcement.¹⁴⁰¹ In Sept. of 2003, a federal jury found a Florida hacker known as “JungleMike” guilty under the DMCA of selling hardware used to illegally receive DirecTV satellite broadcasts. This case marked the first-ever jury conviction under the DMCA. Several other defendants pleaded guilty to DMCA charges in the same operation.¹⁴⁰²

In July of 2005, a Maryland man, one of a group of employees and managers from the three-store Pandora’s Cube chain in Maryland, pled guilty and was sentenced to four months in prison for conspiracy to commit felony copyright infringement and for violating the DMCA based on sales by Pandora’s Cube of modified Xboxes that let players use pirated console games. Pandora’s Cube was also selling modified Xboxes preloaded with pirated games.¹⁴⁰³

¹³⁹⁷ Id. at 1743.

¹³⁹⁸ Id.

¹³⁹⁹ Id. at 1744-57.

¹⁴⁰⁰ Howard Mintz, “Russian Company is Acquitted by S.J. Jury” (Dec. 17, 2002), available as of Dec. 18, 2002 at www.bayarea.com/mld/mercurynews/4763575.htm.

¹⁴⁰¹ Declan McCullagh, “Feds Confiscate ‘Illegal’ Domain Names” (Feb. 26, 2003), available as of Feb. 27, 2003 at www.news.com.com/2102-1023-986225.html.

¹⁴⁰² “DirecTV Hacker Convicted Under DMCA,” *BNA’s Patent, Trademark & Copyright Journal* (Sept. 26, 2003) at 595.

¹⁴⁰³ Daniel Terdiman, “Video Game Pirate Headed to Slammer” (July 27, 2005), available as of July 28, 2005 at http://news.com.com/2100-1043_3-5807547.html.

In United States v. Whitehead,¹⁴⁰⁴ the Ninth Circuit affirmed the sentence for a man who was convicted of selling over \$1 million worth of counterfeit access cards that allowed his customers to access DirecTV's digital satellite feed without paying for it. The court found no abuse of discretion in the district court's conclusion that a substantial amount of community service (1000 hours), a hefty restitution order (\$50,000) and five years of supervised release were more appropriate than prison, even though the punishment was below that of the federal sentencing guidelines, which called for a range of 41 to 51 months in prison.¹⁴⁰⁵

(iii) The Requirement of Willfulness – Deliberate Ignorance

In United States v. Reichert,¹⁴⁰⁶ Reichert appealed his criminal conviction and sentence to jail for twelve months and one day for willful violation of Section 1201(a) for trafficking in circumvention technology by installing a modification chip in a Nintendo Wii so that it could run software for which it was not originally designed and then selling the modified Wii to a federal agent for a \$50 profit. Agents subsequently obtained a search warrant and seized additional modification chips and other items from Reichert's home. Among other things, Reichert challenged the jury instructions on willfulness.¹⁴⁰⁷

The court issued two germane instructions. The first pertained to the issue of willfulness generally:

As used in these instructions, an act is done willfully if it is done voluntarily and intentionally with the intent to do something unlawful, that is, with the intent either to disobey or disregard the law.

While a person must have acted with the intent to do something the law forbids, the person need not be aware of the specific law or the rule his conduct is violating. Willfulness requires the Government to prove that the law imposed a duty on the Defendant, that the Defendant knew of this duty, and that he voluntarily and intentionally violated that duty.¹⁴⁰⁸

The court then gave the following instruction on "deliberate ignorance":

No one can avoid responsibility for a crime by deliberately ignoring the obvious. If you are convinced that the Defendant deliberately ignored a high probability that he was trafficking in technology primarily designed to circumvent technological measures

¹⁴⁰⁴ 532 F.3d 991 (9th Cir. 2008).

¹⁴⁰⁵ Id. at 992.

¹⁴⁰⁶ 747 F.3d 445 (6th Cir. 2014).

¹⁴⁰⁷ Id. at 447-48, 450.

¹⁴⁰⁸ Id. at 450.

designed to effectively control access to a work copyrighted under copyright law, then you may find that he knew he was violating the Digital Millennium Copyright Act.

But to find this, you must be convinced beyond a reasonable doubt that the Defendant was aware of a high probability that he was violating the Digital Millennium Copyright Act, and that the Defendant deliberately closed his eyes to what was obvious.

Carelessness or negligence or foolishness on his part is not the same as knowledge and is not enough to convict.¹⁴⁰⁹

Reichert challenged the deliberate ignorance instruction on two bases. First, he argued that the instruction failed to properly reflect that a defendant is willfully blind only if he took “deliberate action” to avoid actual knowledge. The court rejected this argument, noting that the deliberate ignorance instruction in this case tracked the language of *Sixth Circuit Pattern Criminal Jury Instruction § 2.09*. The pattern instruction explicitly incorporated the requirement that a defendant act “deliberately” to avoid full knowledge, and the Sixth Circuit noted that it had repeatedly held the instruction to be an accurate statement of the law.¹⁴¹⁰

Second, Reichert asserted that the deliberate ignorance instruction eviscerated the DMCA’s willfulness requirement by allowing the jury to convict him upon finding only that he knew that he was trafficking in circumvention technology, rather than after finding that he knew that he was violating the law by trafficking in such technology. Reichert’s argument rested primarily on the first portion of the deliberate ignorance instruction, which stated, “If you are convinced that the Defendant deliberately ignored a high probability that he was trafficking in technology primarily designed to circumvent technological measures designed to effectively control access to a work copyrighted under federal law, then you may find that he knew he was violating the Digital Millennium Copyright Act.” The Sixth Circuit noted that because this part of the instruction seemed to inform the jury that if Reichert deliberately ignored a high probability that he merely engaged in the conduct at issue, then the jury could find that he knew that his conduct violated the DMCA. The Sixth Circuit noted that this part of the instruction could have been more precise.¹⁴¹¹

However, the court noted that, to the extent the challenged portion of the instruction was imprecise, it was not given in a vacuum. Instead, it was sandwiched between two instructions that stated the stricter requirement of willfulness and clarified the challenged language. Immediately before the challenged sentence, the district court had given its instruction on willfulness generally, explaining that an act is willful if done with the intent either to disobey or disregard the law and that the defendant must have acted with the intent to do something the law forbids. And immediately after giving the challenged portion of the deliberate ignorance instruction, the district court had cautioned the jury that, to find Reichert

¹⁴⁰⁹ Id.

¹⁴¹⁰ Id. at 450-51.

¹⁴¹¹ Id. at 451-52.

knew he was violating the DMCA, the jury must be convinced beyond a reasonable doubt that Reichert was aware of a high probability that he was violating the DMCA and that he deliberately closed his eyes to what was obvious. Accordingly, the Sixth Circuit found that, when viewed as a whole, the instructions properly instructed the jury on the issue of willfulness. The Sixth Circuit noted that, having been properly instructed, the jury had found that Reichert constructively knew that his conduct was against the law, given his admissions that he was operating in a “gray” area of the law and was “technically” not supposed to be engaging in his conduct. Because Reichert had not directly challenged the jury’s factual finding in that regard, the court rejected his challenge to his conviction on the basis of the allegedly erroneous jury instructions.¹⁴¹²

(15) Other Uses of the Anti-Circumvention Provisions as a Sword

The RealNetworks and Reimerdes cases suggest how the anti-circumvention provisions of the DMCA might be used as a “sword” in other ways. For example, the manufacturer of a database product that enables users to password protect data files might bring an action under the DMCA against the manufacturer of “cracking” software that enables third parties to bypass or deactivate the password protection on such data files. The manufacturer of the database product might, for example, allege “injury” from the “cracking” software in the form of damage to its reputation as the manufacturer of a “secure” product. Alternatively, if a claim were made against the database product manufacturer by a user alleging injury resulting from the user’s data file being “cracked” by a third party, such claim would provide another basis for the database product manufacturer to allege its own injury from the “cracking” software.

Other examples of attempts at creative use of the anti-circumvention provisions as a sword are the following:

(i) Lexmark International, Inc. v. Static Control Components, Inc.

Lexmark sold toner cartridges for use with its laser printers. The cartridges were of two types: “regular” cartridges that could be refilled and remanufactured freely by third parties, and “prebate” cartridges that could be used only once, and for which the consumer agreed, in the form of a shrinkwrap agreement placed across the top of every prebate cartridge box, to return the used cartridge to Lexmark for remanufacturing and recycling. Lexmark’s printers contained two computer programs – a Printer Engine Program that controlled various printer operations such as paper feed, paper movement, and motor control, and a Toner Loading Program of 37 to 55 bytes, which resided within microchips attached to the toner cartridges and enabled Lexmark printers to approximate the amount of toner remaining in the cartridge.¹⁴¹³

To protect the Printer Engine Programs and Toner Loading Programs, and to prevent unauthorized toner cartridges from being used with Lexmark’s printers, Lexmark’s printers used an authentication sequence that ran each time a toner cartridge was inserted into a Lexmark

¹⁴¹² Id. at 452-53.

¹⁴¹³ Lexmark International, Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943, 948-49 (E.D. Ky. 2003).

printer, the printer was powered on, or whenever the printer was opened and closed. The authentication sequence required the printer and the microchip on the cartridge to calculate a Message Authentication Code (MAC) using a hashing algorithm, to communicate the MAC from the microchip to the printer, and the printer to compare the MAC it calculated with the MAC it received from the microchip. If the MAC calculated by the microchip matched that calculated by the printer, the cartridge was authenticated and authorized for use by the printer, which in turn enabled the Printer Engine Program to allow the printer to print and the Toner Loading Program to monitor the toner status of the authenticated cartridge.¹⁴¹⁴

The defendant Static Control Components (SCC) manufactured and sold a “SMARTEK” microchip that was used to replace the microchip found in Lexmark’s toner cartridges. SCC admitted that it copied verbatim Lexmark’s Toner Loading Program into its SMARTEK microchips and that its SMARTEK microchips were designed to circumvent Lexmark’s authentication sequence by mimicking the sequence performed by an original microchip on Lexmark’s cartridges and the printer.¹⁴¹⁵ Lexmark sued SCC for violation of the anti-circumvention provisions of the DMCA as well as copyright infringement.

The District Court’s Ruling. On a motion for a preliminary injunction, the district court ruled that SCC had violated the anti-circumvention provisions of the DMCA and committed copyright infringement. With respect to the issue of infringement, although SCC admitted copying the Toner Loading Program, SCC argued that the program was not copyrightable because it was a functional “lock-out code” whose exact content was required as part of the authentication sequence. The court rejected this argument, because the binary content of the Toner Loading Program was not used as an input to the hashing algorithm of the authentication sequence, and copying of the Toner Loading Program was therefore not necessary for a valid authentication sequence to occur.¹⁴¹⁶ The court also rejected SCC’s arguments that its copying was a fair use, noting that “[w]here the accused infringer’s copying is part of the ordinary operation of the accused product, fair use does not apply,”¹⁴¹⁷ and that the Toner Loading Program was an uncopyrightable formula or constant, noting that there were a number of ways the Toner Loading Program could have been written to approximate toner level.¹⁴¹⁸ Because SCC had engaged in verbatim copying of the Toner Loading Program, it had committed copyright infringement. The court also rejected a copyright misuse defense, ruling that “Lexmark’s efforts

¹⁴¹⁴ Id. at 952-53.

¹⁴¹⁵ Id. at 955-56.

¹⁴¹⁶ Id. at 950, 958-59.

¹⁴¹⁷ Id. at 960.

¹⁴¹⁸ Id. at 962.

to enforce the rights conferred to it under the DMCA cannot be considered an unlawful act undertaken to stifle competition.”¹⁴¹⁹

Turning to the DMCA claim, the court found that the SMARTEK microchips violated the anti-circumvention provision of Section 1201(a)(2) in that its primary purpose was to circumvent a technological measure that effectively controlled access to a copyrighted work. The court adopted a plain dictionary meaning of “access” as the “ability to enter, to obtain, or to make use of.”¹⁴²⁰ The court held that the authentication sequence was an effective technological measure restricting access under this definition, because it required application of information and the application of a process to gain access to Lexmark’s copyrighted Toner Loading Programs and Printer Engine Programs for use.¹⁴²¹ Accordingly, SCC’s manufacture, distribution and sale of its SMARTEK microchips violated the DMCA.¹⁴²² The court held that the exemption under Section 1201(f) for circumvention for reverse engineering “solely for the purpose of enabling interoperability of an independently created computer program with other programs” was inapplicable. The court ruled that SCC’s SMARTEK microchips could not be considered to contain independently created computer programs, since they were exact copies of Lexmark’s Toner Loading Programs and the “SMARTEK microchips serve no legitimate purpose other than to circumvent Lexmark’s authentication sequence.”¹⁴²³

Finally, the court ruled, consistent with the Reimerdes case, that a plaintiff that demonstrates a likelihood of success on the merits of a claim for violation of the anti-circumvention provisions of the DMCA is entitled to a presumption of irreparable injury for purposes of a preliminary injunction. Accordingly, the court entered a preliminary injunction against the distribution of the SMARTEK microchips.¹⁴²⁴

The Sixth Circuit’s Ruling. On appeal, the Sixth Circuit reversed and remanded.¹⁴²⁵ Turning first to the issue of copyright infringement, the Sixth Circuit found the district court’s ruling erroneous with respect to whether the Toner Loading Program constituted a “lock-out code.” The court noted generally that “[t]o the extent compatibility requires that a particular code sequence be included in [a] component device to permit its use, the merger and scenes a faire doctrines generally preclude the code sequence from obtaining copyright protection.”¹⁴²⁶

¹⁴¹⁹ Id. at 966. The court further noted that an “antitrust claim cannot succeed under an after-market antitrust theory when the accused party has not changed its policy and has been otherwise forthcoming about its policies.” Id. at 966 n.3.

¹⁴²⁰ Id. at 967.

¹⁴²¹ Id. at 967-68.

¹⁴²² Id. at 969-70.

¹⁴²³ Id. at 971.

¹⁴²⁴ Id. at 971, 974.

¹⁴²⁵ Lexmark Int’l v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004), reh’g denied, 2004 U.S. App. LEXIS 27422 (Dec. 29, 2004), reh’g en banc denied, 2005 U.S. App. LEXIS 3330 (6th Cir. Feb. 15, 2005).

¹⁴²⁶ Id. at 536.

The court noted that the Toner Loading Program served as input to a checksum operation performed each time the printer was powered on or the printer door was opened and closed for toner cartridge replacement. Specifically, after downloading a copy of the Toner Loading Program to calculate toner levels, the Printer Engine Program ran the checksum calculation using every data byte of the Toner Loading Program as input. The program then compared the result of the calculation with a checksum value located elsewhere on Lexmark's toner cartridge chip. If any single byte of the Toner Loading Program was altered, the checksum value would not match the checksum calculation result.¹⁴²⁷

In addition, the Sixth Circuit noted that, at least for purposes of a preliminary injunction, the expert testimony established that it would be "computationally impossible" to modify the checksum value without contextual information that the defendant did not have access to. Accordingly, the checksum operation imposed a compatibility constraint that "justified SCC's copying of the Toner Loading Program."¹⁴²⁸ Accordingly, the court concluded that, on the preliminary injunction record, the Toner Loading Program was not copyrightable.¹⁴²⁹

With respect to the DMCA claims, the Sixth Circuit began its analysis by agreeing with the district court and the Reimerdes case that there should be a presumption of irreparable harm arising from demonstration of a likelihood of success on a DMCA claim.¹⁴³⁰ The court then turned to separate analyses of Lexmark's anti-circumvention claims with respect to the Printer Engine Program and the Toner Loading Program.

Concerning the Printer Engine Program, the court held that Lexmark's authentication sequences did not "control access" to the Printer Engine program sufficiently to trigger the applicability of the anti-circumvention provisions because anyone could read the literal code of the Printer Engine Program directly from the printer memory, with or without the benefit of the authentication sequence.¹⁴³¹ "The authentication sequence, it is true, may well block one form of 'access' – the ability to ... make use of' the Printer Engine Program by preventing the printer

¹⁴²⁷ Id. at 541.

¹⁴²⁸ Id. at 542.

¹⁴²⁹ Id. at 544. Because the court found the Toner Loading Program not to be copyrightable, it noted that it need not decide whether copying of the same was a fair use. Nevertheless, the court noted its disagreement with the district court's fair use analysis, among other reasons because the copying was done for functional reasons. "In copying the Toner Loading Program into each of its SMARTEK chips, SCC was not seeking to exploit or unjustly benefit from any creative energy that Lexmark devoted to writing the program code. As in *Kelly*, SCC's chip uses the Toner Loading Program for a different purpose, one unrelated to copyright protection. Rather than using the Toner Loading Program to calculate toner levels, the SMARTEK chip uses the content of the Toner Loading Program's data bytes as input to the checksum operation and to permit printer functionality. Under these circumstances, it is far from clear that SCC copied the Toner Loading Program for its commercial value as a *copyrighted work* – at least on the preliminary-injunction record we have before us." Id.

¹⁴³⁰ Id. at 533.

¹⁴³¹ Id. at 546.

from functioning. But it does not block another relevant form of ‘access’ – the ‘ability to [] obtain’ a copy of the work or to ‘make use of’ the literal elements of the program (its code).”¹⁴³²

The court rejected Lexmark’s argument that several cases had embraced a “to make use of” definition of “access” in applying the DMCA. The court noted that “[i]n the essential setting where the DMCA applies, the copyright protection operates on two planes: in the literal code governing the work and in the visual or audio manifestation generated by the code’s execution.”¹⁴³³ Those cases finding liability based on a technological measure that restricted “use” of the work were ones in which consumers were restricted from making use of copyrightable expression in the work, such as a video game.¹⁴³⁴

“The copyrightable expression in the Printer Engine Program, by contrast, operates on only one plane: in the literal elements of the program, its source and object code. Unlike the code underlying video games or DVDs, ‘using’ or executing the Printer Engine Program does not in turn create any protected expression. Instead, the program’s output is purely functional. ... Presumably, it is precisely because the Printer Engine Program is not a conduit to protectable expression that explains why Lexmark (or any other printer company) would not block access to the computer software that makes the printer work. Because Lexmark’s authentication sequence does not restrict access to this literal code, the DMCA does not apply.”¹⁴³⁵

The Sixth Circuit’s holding that, to qualify for DMCA anti-circumvention protection, a technological measure for a computer program must block either the ability to copy the code or to read the literal code, at least where that code does not create any separately protectable expression such as a video game, is potentially very significant. Many computer programs perform only “invisible” functions and do not generate copyrightable expression as output to the user. The Sixth Circuit’s ruling that technological measures which merely restrict use of such programs, and do not prohibit copying or reading of the code (such as passwords and handshaking or other authentication sequences), do not qualify for anti-circumvention protection under the DMCA, if adopted by other courts and applied widely, may significantly narrow the scope of protection the DMCA affords to computer programs. Under the Sixth Circuit’s definition of “access control,” it may be that only those measures that encrypt or otherwise protect a program against copying or the ability to read it will be sufficient to qualify purely “functional” programs for anti-circumvention protection under the DMCA.

Concerning the Toner Loading Program, the court ruled that the defendant’s chip did not provide “access” to the Toner Loading Program, but rather replaced the program, and therefore did not circumvent any access control. In addition, to the extent the Toner Loading Program was

¹⁴³² *Id.* at 547 (quoting from *Merriam-Webster’s Collegiate Dictionary*’s definitions of “access”).

¹⁴³³ *Id.* at 548.

¹⁴³⁴ *Id.*

¹⁴³⁵ *Id.*

not copyrightable, it would not constitute a “work protected under [the copyright statute]” to which the DMCA protections would apply.¹⁴³⁶

Finally, the court turned to the interoperability defenses asserted by the defendant. The Sixth Circuit rejected the district court’s ruling against the defendant’s argument that its microchip constituted a “technological means” that it could make available to others under § 1201(f)(3) solely for the purpose of enabling interoperability of an independently created computer program with other programs. The district court rejected the defense on the ground that the defendant had copied the Toner Loading Program and thus had not created an independently created computer program.¹⁴³⁷

The Sixth Circuit noted that, even if the Toner Loading Program had been copied, the defendant’s microchips contained other independently developed computer programs that interoperated with the Printer Engine Program, and those other programs were sufficient to allow the defendant to benefit from the interoperability defense.¹⁴³⁸ The implication of this ruling is that every computer program on a device need not qualify for the interoperability defense in order for the device itself to be able to benefit from the defense.

The court also rejected Lexmark’s argument that the independently created program must have existed prior to the reverse engineering – holding that they can be created simultaneously – and its argument that the circumvention means must be necessary or absolutely needed for interoperability – ruling that the statute is silent as to whether there is any necessity requirement at all, but there was necessity in this case because the Toner Loading Program was used in a checksum calculation. Finally, the defendant’s copying of the Toner Loading Program did not destroy the interoperability defense (§ 1201(f)(3) conditions its defense on a requirement that the circumvention not violate other “applicable law”) because the Sixth Circuit had concluded that the Toner Loading Program was not copyrightable on the preliminary injunction record.¹⁴³⁹ Accordingly, the Sixth Circuit vacated the district court’s grant of a preliminary injunction and remanded the case.¹⁴⁴⁰

The depth of the court’s concern about the policy implications of Lexmark’s proposed broad reading for the scope of the anti-circumvention provisions is further illustrated by comments made by two members of the panel in separate opinions. One judge, in a concurring opinion, noted that the main point of the DMCA is “to prohibit the pirating of copyright-protected works such as movies, music and computer programs. If we were to adopt Lexmark’s reading of the statute, manufacturers could potentially create monopolies for replacement parts

¹⁴³⁶ *Id.* at 549-50.

¹⁴³⁷ *Id.* at 550.

¹⁴³⁸ *Id.*

¹⁴³⁹ *Id.* at 550-51.

¹⁴⁴⁰ *Id.* at 551.

simply by using similar, but more creative, lock-out codes.”¹⁴⁴¹ He further stated that “Congress did not intend to allow the DMCA to be used offensively in this manner, but rather only sought to reach those who circumvented protective measures ‘for the purpose’ of pirating works protected by the copyright statute.”¹⁴⁴²

Another judge, in an opinion concurring in part and dissenting in part, stated, “We agree that the DMCA was not intended by Congress to be used to create a monopoly in the secondary markets for parts or components of products that consumers have already purchased.”¹⁴⁴³ This judge also argued that fair use should be a defense to an anti-circumvention violation, because where fair use applies there would be no “right of a copyright owner” to be infringed by the circumvention.¹⁴⁴⁴

By order entered Feb. 23, 2006, the parties stipulated to entry of summary judgment on all DMCA claims and counterclaims in favor of Static Control Components. The order preserved Lexmark’s right to appeal the order, as well as the Sixth Circuit’s interpretation of the DMCA, after entry of final judgment on all issues in the cases.¹⁴⁴⁵

On remand from the Sixth Circuit, the district court found that neither party had submitted new evidence that would undermine the Sixth Circuit’s applicability of facts to the law with respect to the issue of the copyrightability of the Toner Loader Program. Accordingly, the Sixth Circuit’s decision controlled, and the court ruled that the Toner Loader Program was insufficiently original to be copyrightable.¹⁴⁴⁶ The court also held that, even if the Toner Loader Program were copyrightable, the defendant’s use of it on its chip was a fair use, principally on the ground that the first fair use factor weighed heavily in the defendant’s favor “because Lexmark does not even rebut that [the defendant’s] purpose for copying the [Toner Loader Program] was solely for the purpose of enabling interoperability between remanufactured Lexmark cartridges and Lexmark printers, *not* for the allegedly-expressive, hypothetically-copyrightable content contained therein.”¹⁴⁴⁷

¹⁴⁴¹ Id. at 552.

¹⁴⁴² Id.

¹⁴⁴³ Id. at 553. The judge also noted a link in the legislative history between the anti-circumvention prohibitions and the facilitation of copyright infringement. He quoted a House Report to the DMCA stating that Section 1201(b)(1) sought to prohibit “making or selling the technological means to overcome these protections and *thereby facilitate copyright infringement.*” Id. at 564 (emphasis by the court) (quoting H.R. Rep. 105-796 (Oct. 8, 1998)).

¹⁴⁴⁴ 387 F.3d at 562.

¹⁴⁴⁵ See “Lexmark Stipulates to Judgment on DMCA Claims,” *BNA’s Patent, Trademark & Copyright Journal* (Mar. 10, 2006) at 506.

¹⁴⁴⁶ Static Control Components, Inc. v. Lexmark Int’l, Inc., 2007 U.S. Dist. LEXIS 36017 at *36 (E.D. Ky. Apr. 18, 2007).

¹⁴⁴⁷ Id. at *38.

(ii) **Chamberlain Group, Inc. v. Skylink Technologies, Inc.**

In this case, the plaintiff Chamberlain was the manufacturer of a garage door opener (GDO) system which contained a feature known as “rolling code” designed to protect against burglars equipped with “code grabber” devices. A code grabber allows a burglar to capture and record the coded radio frequency (RF) signal sent by the transmitter device to the GDO, which can then be used to open the GDO at a later time to enter the house.¹⁴⁴⁸ Chamberlain’s rolling code feature was designed to defeat code grabbers by changing the expected transmitted RF code each time the GDO was activated. The feature was implemented by two copyrighted computer programs owned by Chamberlain – one in the transmitter of the GDO and the other in the receiver of the GDO that activated the motor to open the door. Each time the transmitter was activated to open the door, the computer program in the transmitter would cause the next rolling code in sequence to be sent to the receiver where it was stored, which code the receiver would require the next time the transmitter was activated, or the door would not open.¹⁴⁴⁹

The defendant sold a universal transmitter device that was capable of opening Chamberlain’s GDO, although the opener code transmitted by the defendant’s door opener was not a rolling code. The defendant’s door opener was able to bypass Chamberlain’s rolling code feature by mimicking a certain “resynchronization” process of Chamberlain’s rolling code software.¹⁴⁵⁰ Chamberlain characterized that portion of the computer program in the receiver that verified the rolling code as a protective measure that controlled access to Chamberlain’s copyrighted computer program in the receiver, and argued that by circumventing the rolling code feature and gaining access to the receiver computer program to open the garage door, the defendant was in violation of the anti-circumvention provisions of Section 1201(a)(2).¹⁴⁵¹

Rulings by the District Court. The district court denied a motion by Chamberlain for summary judgment on the anti-circumvention claim, analyzing a number of defenses raised by the defendant. The first defense was that because the defendant’s universal transmitter was capable of operating a number of different GDOs, it was not “primarily” designed to circumvent the access control measure of Chamberlain’s GDO. The court rejected this argument, noting that the defendant’s transmitter had one particular setting that served only one function – to operate the Chamberlain rolling code GDO. The fact that the transmitter was able to serve more than one purpose was insufficient to deny summary judgment to Chamberlain.¹⁴⁵²

Next, the defendant argued that Chamberlain’s computer programs were not in fact subject to copyright protection. The court ruled that this argument raised a disputed issue of material fact sufficient to deny summary judgment, particularly since Chamberlain had not

¹⁴⁴⁸ Chamberlain Group Inc. v. Skylink Technologies Inc., 292 F. Supp. 2d 1023, 1026-27 (N.D. Ill. 2003).

¹⁴⁴⁹ Id. at 1027-28.

¹⁴⁵⁰ Id. at 1029-32.

¹⁴⁵¹ Id. at 1028, 1033.

¹⁴⁵² Id. at 1037-38.

supplied to the defendant the most recent version of the rolling code software until filing its reply brief (which differed from the version of the software that Chamberlain had registered), and the defendant had therefore not had a sufficient opportunity to review it.¹⁴⁵³

Finally, the defendant argued that the consumers' use of the defendant's transmitter with Chamberlain's rolling code GDOs was authorized. In particular, Chamberlain argued that a consumer who purchases a Chamberlain GDO owns it and has a right to use it to access his or her own garage. Before the defendant's transmitter was capable of operating the rolling code GDO, the consumer was required to program the transmitter into the GDO. The defendant argued that this fact demonstrated that the consumer had thereby authorized the use of the defendant's transmitter with the GDO software. The defendant further noted that the packaging for Chamberlain's GDO did not include any restrictions on the consumer's ability to buy a replacement transmitter or additional transmitter.¹⁴⁵⁴ Thus, according to the defendant, "those Chamberlain GDO consumers who purchase a Skylink transmitter are not accessing the GDO without the authority of Chamberlain, but instead, have the tacit permission of Chamberlain to purchase any brand of transmitter that will open their GDO."¹⁴⁵⁵ The court ruled that these facts, together with the fact that there was a history in the GDO industry of universal transmitters being marketed and sold to allow homeowners an alternative means to access any brand of GDO, raised sufficient disputes of material fact about whether the owner of a Chamberlain rolling code GDO was authorized to use the defendant's universal transmitter to deny summary judgment to Chamberlain.¹⁴⁵⁶

Following this opinion, and at the invitation of the court, the defendant moved for summary judgment on Chamberlain's DMCA claim, which the court granted.¹⁴⁵⁷ Although both parties had agreed for purposes of Chamberlain's original motion for summary judgment that Chamberlain did not place any restrictions on consumers regarding the type of transmitter they had to buy to operate a Chamberlain rolling code GDO, in opposing the defendant's motion for summary judgment, Chamberlain submitted an affidavit of its Vice President asserting that Chamberlain did not authorize the circumvention of its rolling code GDOs, and argued that it had not warned consumers against using unauthorized transmitters because it had no idea that

¹⁴⁵³ Id. at 1038.

¹⁴⁵⁴ Id. at 1039.

¹⁴⁵⁵ Id.

¹⁴⁵⁶ Id. at 1040. An amicus brief submitted by the Computer and Communications Industry Association (CCIA) argued that the court should deny summary judgment because the defendant's activities fell within Section 1201(f) of the DMCA, which CCIA argued permits circumvention of a protective measure for the purpose of achieving interoperability. The court noted that, although it was not reaching this issue, the defendant might perhaps be entitled to summary judgment on that basis. Id.

¹⁴⁵⁷ Chamberlain Group, Inc. v. Skylink Technologies, Inc., 292 F. Supp. 2d 1040 (N.D. Ill. 2003). As a preliminary matter, Chamberlain asserted that the defendant bore the burden of proof to show that it was authorized to circumvent – not access – Chamberlain's software as an affirmative defense. The court disagreed, ruling that it was clearly Chamberlain's burden to demonstrate that the defendant circumvented a technological measure without the authority of the copyright owner. Id. at 1044.

other transmitters could be made to operate its rolling code GDOs.¹⁴⁵⁸ The court rejected these arguments, finding that the affidavit was conclusory and entitled to little weight, and that Chamberlain’s failure to anticipate the defendant’s technology did not “refute the fact that homeowners have a reasonable expectation of using the technology now that it is available.”¹⁴⁵⁹

Finally, Chamberlain argued that even if its customers were authorized to circumvent its security measures, that had no bearing on whether sellers had similar authorization. The court found this argument ignored the fact that (1) there was a history in the GDO industry of marketing and selling universal transmitters; (2) Chamberlain had not placed any restrictions on the use of competing transmitters to access its rolling code GDOs; and (3) in order for the defendant’s transmitter to activate the Chamberlain garage door, the homeowner herself had to choose to store the defendant’s transmitter signal into the Chamberlain GDO’s memory, thereby demonstrating the homeowner’s willingness to bypass Chamberlain’s system and its protections.¹⁴⁶⁰

Accordingly, the court granted the defendant’s motion for partial summary judgment with respect to Chamberlain’s DMCA claim.¹⁴⁶¹ Since so much of the district court’s opinion emphasized the fact that Chamberlain had not placed restrictions on the type of transmitters customers could use to operate Chamberlain’s GDOs, one must wonder whether the court would have ruled differently had Chamberlain made clear to customers of its GDO products at the time of purchase that they were not authorized to use any transmitters to access the software in their GDOs other than Chamberlain’s transmitters. If so, then under the district court’s rationale, it seems that DMCA claims of the type Chamberlain made in this case could easily be strengthened by copyright holders in the future by making express statements of authorization with respect to use of their products. The Federal Circuit, in its decision on appeal, expressly declined to reach this issue.¹⁴⁶²

The Federal Circuit’s Decision. On appeal, the Federal Circuit affirmed in a detailed opinion that examined the legislative history and purpose of the anti-circumvention provisions of the DMCA, and placed some significant boundaries around the scope of those provisions.¹⁴⁶³ The Federal Circuit began its analysis by ruling that the plaintiff has the burden under an anti-circumvention claim to prove that the defendant’s access to its copyrighted work was not authorized. The court derived this holding from the distinction between a copyright – which is a property right – and the anti-circumvention provisions – which do not establish a new property

¹⁴⁵⁸ Id.

¹⁴⁵⁹ Id.

¹⁴⁶⁰ Id. at 1946.

¹⁴⁶¹ Id.

¹⁴⁶² The Federal Circuit did, however, make some statements suggesting that such restrictions might constitute copyright misuse, as discussed below.

¹⁴⁶³ The Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir. 2004)), cert. denied, 161 L. Ed. 2d 481 (2005).

right, but rather only a new cause of action for liability. Under a copyright (a property right), the plaintiff need only establish copying, and the burden then shifts to the defendant to prove a defense. By contrast, under the anti-circumvention provisions, the language of the statute defines the cause of action in terms of a circumvention or trafficking without authority of the copyright owner. The plaintiff therefore has the burden to prove that the defendant's access was unauthorized.¹⁴⁶⁴

In a very significant ruling, the Federal Circuit held that the anti-circumvention provisions of Section 1201 do not apply to all forms of circumvention to gain access to a work, but rather only to circumventions that accomplish "forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners"¹⁴⁶⁵ – in other words, circumventions that facilitate some form of copyright infringement.¹⁴⁶⁶ Conversely, "defendants whose circumvention devices do not facilitate infringement are not subject to § 1201 liability."¹⁴⁶⁷

The court reached this conclusion based on three rationales. First, the court noted that in the statutory language itself, "virtually every clause of § 1201 that mentions 'access' links 'access' to 'protection.'"¹⁴⁶⁸ Second, the court found that every decision cited by the plaintiff finding anti-circumvention liability involved a circumvention that facilitated or was coupled with copyright infringement. In the Reimerdes case, the DeCSS program allowed the user to circumvent the CSS protective system and to view or to copy a motion picture from a DVD, whether or not the user had a DVD player with the licensed technology. In the Lexmark case, the court ruled that the defendant's conduct in copying the Toner Loading Program constituted copyright infringement. In the Gamemasters case, the defendant conceded that its product made temporary modifications to the plaintiff's copyrighted computer program. In the Real Networks case, the defendant's product allegedly disabled Real Networks' copy switch, which defeated the copyright owner's ability to control copying upon streaming of the work.¹⁴⁶⁹ "In short, the access alleged in all [these] cases was intertwined with a protected right."¹⁴⁷⁰

Third, the court believed that a broad reading of the anti-circumvention provisions to prohibit all forms of unauthorized access, whether or not protected copyright rights were thereby implicated, as urged by Chamberlain, would risk too much potential harm to competition. "Chamberlain's proposed construction would allow any manufacturer of any product to add a single copyrighted sentence or software fragment to its product, wrap the copyrighted material in a trivial 'encryption' scheme, and thereby gain the right to restrict

¹⁴⁶⁴ Id. at 1193.

¹⁴⁶⁵ Id. at 1202.

¹⁴⁶⁶ Id. at 1195, 1203.

¹⁴⁶⁷ Id. at 1195.

¹⁴⁶⁸ Id. at 1197.

¹⁴⁶⁹ Id. at 1198-99 (citations omitted).

¹⁴⁷⁰ Id. at 1199.

consumers' rights to use its products in conjunction with competing products. In other words, Chamberlain's construction of the DMCA would allow virtually any company to attempt to leverage its sales into aftermarket monopolies – a practice that both the antitrust laws and the doctrine of copyright misuse normally prohibit.”¹⁴⁷¹

The court noted that such a broad reading would also contradict other statutory provisions of the DMCA. In particular, Section 1201(c)(1) provides that nothing in Section 1201 shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use. The court noted that a reading of Section 1201 that prohibited access without regard to the rest of the copyright statute would clearly affect rights and limitations, if not remedies and defenses,¹⁴⁷² and might also be tantamount to “ignoring the explicit immunization of interoperability from anticircumvention liability under § 1201(f).”¹⁴⁷³

The court's statements might imply that circumvention for fair uses is privileged. Indeed, the court stated, “Chamberlain's proposed construction would allow copyright owners to prohibit exclusively fair uses even in the absence of any feared foul use. It would therefore allow any copyright owner, through a combination of contractual terms and technological measures, to repeal the fair use doctrine with respect to an individual copyrighted work – or even selected copies of that copyrighted work. Again, this implication contradicts § 1201(c)(1) directly.”¹⁴⁷⁴ Despite these pregnant statements, however, the court stated in a footnote, “We leave open the question as to when § 107 might serve as an affirmative defense to a prima facie violation of § 1201. For the moment we note only that though the traditional fair use doctrine of § 107 remains unchanged as a defense to copyright infringement under § 1201(c)(1), circumvention is not infringement.”¹⁴⁷⁵

Turning to Chamberlain's specific claims under Section 1201(a)(2), the court summarized the requirements for liability as follows:

A plaintiff alleging a violation of § 1201(a)(2) must prove: (1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, (3) that third parties can now access (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other

¹⁴⁷¹ *Id.* at 1201 (citations omitted).

¹⁴⁷² *Id.* at 1200.

¹⁴⁷³ *Id.* Although amicus Computer and Communications Industry Association urged the court to consider the import of Section 1201(f) on the case, the court did not reach the issue since it held there had been no anti-circumvention violation by the defendant in the first place under its reading of the scope of the DMCA. *Id.* at 1191 n.8.

¹⁴⁷⁴ *Id.* at 1202.

¹⁴⁷⁵ *Id.* at 1200 n.14.

than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure.¹⁴⁷⁶

The court ruled that Chamberlain had failed to satisfy both the fourth and fifth elements of the test. With respect to the fifth element, Chamberlain had neither alleged copyright infringement nor explained how the access provided by the defendant's transmitter facilitated third party infringement of any of its copyright rights. Instead, the defendant's transmitter merely enabled the end user to make legitimate use of the computer program in the GDO.¹⁴⁷⁷

Nor had Chamberlain established the fourth element. The record established that Chamberlain had placed no explicit restrictions on the types of transmitter that the homeowner could use with its system at the time of purchase.¹⁴⁷⁸ "Copyright law itself authorizes the public to make certain uses of copyrighted materials. Consumers who purchase a product containing a copy of embedded software have the inherent legal right to use that copy of the software. What the law authorizes, Chamberlain cannot revoke."¹⁴⁷⁹ Although this statement suggests that a plaintiff could not even use contractual prohibitions to eliminate authorization to circumvent controls to gain access to the software in a way that did not facilitate infringement, the court backed away from any such absolute principle in a footnote: "It is not clear whether a consumer who circumvents a technological measure controlling access to a technological measure controlling access to a copyrighted work in a manner that enables uses permitted under the Copyright Act but prohibited by contract can be subject to liability under the DMCA. Because Chamberlain did not attempt to limit its customers' use of its product by contract, however, we do not reach that issue."¹⁴⁸⁰

In conclusion, then, the court held, "The Copyright Act authorized Chamberlain's customers to use the copy of Chamberlain's copyrighted software embedded in the GDOs that they purchased. Chamberlain's customers are therefore immune from § 1201(a)(1) circumvention liability. In the absence of allegations of either copyright infringement or § 1201(a)(1) circumvention, Skylink cannot be liable for § 1201(a)(2) trafficking."¹⁴⁸¹ The court therefore affirmed the district court's grant of summary judgment in favor of Skylink.¹⁴⁸²

¹⁴⁷⁶ Id. at 1203.

¹⁴⁷⁷ Id. at 1198, 1204.

¹⁴⁷⁸ Id. at 1183.

¹⁴⁷⁹ Id. at 1202.

¹⁴⁸⁰ Id. at 1202 n.17.

¹⁴⁸¹ Id. at 1204.

¹⁴⁸² Id.

(iii) In re Certain Universal Transmitters for Garage Door

Openers

In addition to its lawsuit against Skylink, Chamberlain also filed an action in the International Trade Commission to bar the importation of Skylink's GDOs. That investigation established a second ground beyond that of the district court's ruling as to why Skylink had not committed a violation of the DMCA. Specifically, in an Initial Determination concerning temporary relief in the investigation that preceded the district court's ruling, an administrative law judge denied temporary relief on the ground that Skylink's transmitters did not violate the DMCA because they "do not circumvent Chamberlain's copyrighted rolling code software program, but instead send fixed identification code signals to Chamberlain's GDOs that fall outside of the copyrighted software. ... The fact that [Skylink's] transmitters send a fixed identification code that does not circumvent Chamberlain's copyrighted software program removes those products entirely from the purview of the DMCA, regardless of whether Chamberlain warns its customers and Skylink that non-rolling code transmitters are unauthorized."¹⁴⁸³

After the district court's ruling, Skylink moved to dismiss the ITC investigation on the ground that Chamberlain's claim was barred under res judicata by that ruling. Chamberlain opposed the dismissal on the ground that there were new facts not before the district court – namely, that Chamberlain had since changed its GDO users' manuals to expressly warn customers that use of non-rolling code transmitters would circumvent Chamberlain's rolling code security measure, and to make clear that customers were not authorized to access Chamberlain's operating software using non-rolling code transmitters.¹⁴⁸⁴ The administrative law judge ruled that this fact was insufficient to avoid res judicata, because the fact could have been asserted before the district court, since the administrative ruling on the request for temporary relief issued before the district court acted.¹⁴⁸⁵ In addition, the administrative law judge ruled that Chamberlain's new owners' manuals "impose no enforceable restrictions on consumers even if they do 'warn' them that non-rolling code transmitters are 'unauthorized.' There are no negative consequences for a consumer who ignores the statement in Chamberlain's new manuals."¹⁴⁸⁶ Accordingly, the administrative law judge determined that the investigation should be terminated in its entirety and certified that determination to the Commission.¹⁴⁸⁷

¹⁴⁸³ In re Certain Universal Transmitters for Garage Door Openers, 70 U.S.P.Q.2d 1906, 1909 (I.T.C. 2004).

¹⁴⁸⁴ Id. at 1907-08.

¹⁴⁸⁵ Id. at 1909-10.

¹⁴⁸⁶ Id. at 1910.

¹⁴⁸⁷ Id.

(iv) Storage Technology Corporation v. Custom Hardware
Engineering & Consulting

In this case, the plaintiff Storage Technology Corporation (“StorageTek”) sold systems for storing and retrieving very large amounts of computer data. StorageTek also serviced its customers’ installations by means of diagnostic software, called the “Maintenance Code,” that it used to identify malfunctions and problems in its customers’ storage systems. In order to protect its service market, StorageTek restricted access to the Maintenance Code with a proprietary algorithm called GetKey.¹⁴⁸⁸

When activated, the Maintenance Code ran a series of diagnostic tests and provided information concerning the nature of existing or potential problems. It was programmed to be set at different levels between 0 and 9. At the 0 level (the usual setting), the Maintenance Code was disabled. Above 0 the Maintenance Code activated specific diagnostic functions at different levels. To enable the Maintenance Code for a particular system, a technician was required to contact StorageTek’s technical support staff, provide the serial number of the equipment being serviced and identify the desired level of the Maintenance Code. The technician would then be given a GetKey password specific to the request that the technician was required to enter in order to reset the maintenance level. During the process of accessing the Maintenance Code and changing the level, a complete copy of the code was made in the RAM memory of the system.¹⁴⁸⁹

The defendants competed with StorageTek for servicing StorageTek systems. They figured out how to circumvent the GetKey algorithm to gain access to the Maintenance Code and to reset its maintenance level in order to run diagnostics that would generate information needed to service a particular system. StorageTek sued for both copyright infringement and violation of the anti-circumvention provisions.¹⁴⁹⁰

The district court held that the defendants had infringed StorageTek’s copyright in the Maintenance Code by virtue of the copy thereof made in RAM each time the GetKey process was circumvented and the maintenance level reset.¹⁴⁹¹ The court held that such copying was not permitted under Section 117(c) of the copyright statute, which provides that it is not an infringement for the owner or lessee of a machine to authorize the making of a copy of a computer program if the program is copied solely by turning on the machine for the purpose only of maintenance and repair and the copy is used in no other manner and is destroyed immediately after the maintenance and repair is completed. The court ruled that Section 117(c) was not available because, although the defendants copied the Maintenance Code by turning on the machine, they did not do so just for repair, but also for the express purpose of circumventing

¹⁴⁸⁸ Storage Technology Corp. v. Custom Hardware Engineering & Consulting, 2004 U.S. Dist. LEXIS 12391 (D. Mass. July 2, 2004) at *3-4.

¹⁴⁸⁹ Id. at *7-8.

¹⁴⁹⁰ Id. at *9-11.

¹⁴⁹¹ Id. at *11-12.

StorageTek's security measures, modifying the maintenance level, and intercepting the diagnostic messages, and they did not destroy the copies they made immediately after completion of repairs.¹⁴⁹²

The court also found a violation of the anti-circumvention provisions of the DMCA, ruling that GetKey was unquestionably a qualifying access control measure and there was no question that the defendants bypassed GetKey. The court also rejected the defendants' reliance on Section 1201(f), because that defense exempts circumvention only if it does not constitute infringement, and the defendants' bypassing of GetKey resulted in an infringing copy of the program being made in RAM.¹⁴⁹³ Accordingly, the court issued a preliminary injunction against the defendants.

On appeal, the Federal Circuit reversed, principally on the ground that the district court's analysis of Section 117(c) was incorrect. The court found that the district court had erred by focusing on the term "repair" in Section 117(c), while ignoring the term "maintenance," which the court noted from the legislative history was meant to encompass monitoring systems for problems, not simply fixing a single, isolated malfunction.¹⁴⁹⁴ The defendant had created software, known as the Library Event Manager (LEM) and the Enhanced Library Event Manager (ELEM) to intercept and interpret fault symptom codes produced by the plaintiff's Maintenance Code.¹⁴⁹⁵ The plaintiff's expert testified that a copy of the Maintenance Code remained in RAM on an ongoing basis as the system operated with the LEM and ELEM attached. Because that description did not comport with the notion of "repair," the district court had ruled Section 117(c) inapplicable. However, in describing the defendants' process, the expert noted that the LEM and ELEM stayed in place so that when problems occurred, the defendants could detect and fix the malfunction. The Federal Circuit ruled that this ongoing presence to detect and repair malfunctions fell within the definition of "maintenance" in Section 117(c). Moreover, when the defendants' maintenance contract was over, the storage library was rebooted, which destroyed the Maintenance Code. The court noted that the protection of Section 117 does not cease simply by virtue of the passage of time, but rather ceases only when maintenance ends.¹⁴⁹⁶

With respect to whether the Maintenance Code was necessary for the machine to be activated, the Federal Circuit relied heavily on the fact that both parties agreed the Maintenance Code was "so entangled with the functional code that the entire code must be loaded into RAM for the machine to function at all."¹⁴⁹⁷ The fact that the Maintenance Code had other functions,

¹⁴⁹² Id. at *12-13.

¹⁴⁹³ Id. at *14-15.

¹⁴⁹⁴ Storage Technology Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307, 1312 (Fed. Cir. 2005), reh'g denied, 431 F.3d 1374 (Fed. Cir. 2005).

¹⁴⁹⁵ Id. at 1310.

¹⁴⁹⁶ Id. at 1313.

¹⁴⁹⁷ Id. at 1314.

such as diagnosing malfunctions in the equipment, was irrelevant. Accordingly, the defendants were likely to prevail on their argument that Section 117(c) protected their act of copying of the plaintiff's Maintenance Code into RAM.¹⁴⁹⁸

Turning to the anti-circumvention claim based on the defendants' circumvention of the GetKey protocol, the court cited its earlier opinion in the Chamberlain case for the proposition that a "copyright owner alleging a violation of section 1201(a) ... must prove that the circumvention of the technological measure either 'infringes or facilitates infringing a right protected by the Copyright Act.'" ¹⁴⁹⁹ Thus, to the extent that the defendants' activities did not constitute copyright infringement or facilitate copyright infringement, the plaintiff was foreclosed from maintaining an action under the DMCA. ¹⁵⁰⁰ Citing the Lexmark and RealNetworks v. Streambox cases, the court observed that "courts generally have found a violation of the DMCA only when the alleged access was intertwined with a right protected by the Copyright Act. ... To the extent that StorageTek's rights under copyright law are not at risk, the DMCA does not create a new source of liability."¹⁵⁰¹

Even if the plaintiff were able to prove that the automatic copying of the Maintenance Code into RAM constituted copyright infringement, it would still have to show that the LEM or ELEM (which bypassed GetKey) facilitated that infringement. With respect to that issue, the court noted the problem that the copying of the Maintenance Code into RAM took place regardless of whether the LEM or ELEM was used. Thus, there was no nexus between any possible infringement and the use of the LEM and ELEM circumvention devices. Rather, the circumvention of GetKey only allowed the defendants to use portions of the copyrighted software that the plaintiff wished to restrict technologically, but that had already been loaded into RAM. "The activation of the maintenance code may violate StorageTek's contractual rights vis-à-vis its customers, but those rights are not the rights protected by copyright law. There is simply not a sufficient nexus between the rights protected by copyright law and the circumvention of the GetKey system."¹⁵⁰² Accordingly, it was unlikely that the plaintiff would

¹⁴⁹⁸ Id. In the alternative, the court ruled that the defendants' copying of the software into RAM was within the software license rights of their customers because the defendants were acting as their customers' agents in turning on the machines. Id. at 1315. "Because the whole purpose of the license is to allow the tape library owners to activate their machines without being liable for copyright infringement, such activity by the licensee and its agents is implicitly authorized by the license agreement unless the agreement explicitly prohibits third parties from powering up the machines." Id. at 1317.

¹⁴⁹⁹ Id. at 1318 (quoting Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004)).

¹⁵⁰⁰ Storage Technology, 421 F.3d at 1318.

¹⁵⁰¹ Id.

¹⁵⁰² Id. at 1319.

prevail on its anti-circumvention claim.¹⁵⁰³ The court therefore vacated the preliminary injunction and remanded for further proceedings.¹⁵⁰⁴

Two significant aspects of the Storage Tech case are worth noting:

– First, the court read the Section 117(c) rights very broadly. Section 117(c) was clearly designed to absolve maintenance providers from copyright liability based merely on the making of a copy of a computer program by virtue of its getting loaded into RAM upon starting a computer for maintenance. However, the Federal Circuit went further, and ruled that the defendants were entitled to *use*, in aid of rendering maintenance, any software that got loaded into RAM upon activation of the machine. Such a result seems in tension with Section 117(c)(2), which provides that, “with respect to any computer program or part thereof that is not necessary for the machine to be activated, such program or part thereof is not accessed or used other than to make such new copy by virtue of the activation of the machine.” The reference to “part thereof” seems to contemplate that some code might get loaded upon machine activation, but yet not be necessary for the machine to be activated (in the way, for example, that operating system software is necessary for a machine to be activated). In that event, Section 117(c)(1) absolves the maintenance provider from liability for the making of the copy of such code upon machine activation, but Section 117(c)(2) would seem to prevent the maintenance provider from accessing or *using* such code “other than to make such new copy by virtue of the activation of the machine.”

Notwithstanding this, the Federal Circuit’s decision gave the maintenance provider the right to access and use the Maintenance Code, just because it was loaded upon activation. The court did so on the articulated basis that the Maintenance Code was “so entangled with the functional code that the entire code must be loaded into RAM for the machine to function at all.”¹⁵⁰⁵ However, this factual assertion seems belied by the fact that, as noted by the district court, the default setting for the Maintenance Code was level 0 (disabled), and it was designed to require intervention by Storage Tech engineers through the GetKey process to activate it to higher levels. Thus, although the Maintenance Code was loaded upon machine activation, it would not seem necessary for the machine to activate (function), because it was by default set to be disabled.

– Second, the court’s interpretation of the anti-circumvention provisions gives them a narrower scope than the literal language of the copyright statute seems to read. Specifically, the court ruled that those provisions do not create a new source of liability beyond copyright infringement. If a circumvention does not lead to a copyright infringement, the circumvention is not illegal. In other words, the act of circumvention is not a *malum in se*.¹⁵⁰⁶ This holding,

¹⁵⁰³ Id.

¹⁵⁰⁴ Id. at 1321.

¹⁵⁰⁵ Id. at 1314.

¹⁵⁰⁶ Latin for “wrong in itself.”

whatever merit it might be argued to have as a policy matter, seems contrary to the literal language of Section 1201(a)(1)(A), which states “No person shall circumvent a technological measure that effectively controls access to a work protected under this title.” The Federal Circuit’s decision seems to add a clause at the end of this provision reading “and which circumvention results in copyright infringement.” As discussed in Section II.G.1(n)(1) above, the separate opinions of two of the judges in the Lexmark case expressed similar views about what the proper scope of the anti-circumvention prohibitions should be interpreted to be.

On remand, StorageTek asserted an additional anti-circumvention claim against the defendants, based on the defendants’ alleged circumvention of GetKey in order to access and copy StorageTek’s Run Time Diagnostics (RTD) code, which diagnosed troubles in the hardware. Unlike the rest of the Maintenance Code, the RTD code was not automatically loaded upon power-up, but instead was loaded only when utilized.¹⁵⁰⁷ The court rejected this claim on the ground that GetKey did not effectively protect or control access to the RTD code. The RTD code was contained on either the hard drive of the LMU or on floppy disks that StorageTek sometimes shipped with its products. Accordingly, any customer who owned a StorageTek system could access and copy the RTD code, regardless of the existence of GetKey protections. The court therefore concluded that GetKey did not effectively control access to the RTD code, and the court granted the defendants summary judgment on the anti-circumvention claim related to the RTD code.¹⁵⁰⁸

(16) Whether Fair Use Constitutes a Defense to Section 1201

On the question whether fair use is a defense to claims under Section 1201, there is an argument that one should distinguish between Sections 1201(a) and 1201(b). Although Sections 1201(a)(2) and 1201(b) in combination prohibit devices designed to circumvent both technological measures that control access to a copyrighted work and that protect a right of a copyright owner, Section 1201(a)(1) prohibits conduct that is directed only to the former, but not the latter. The rationale for this distinction was apparently a belief that anyone should be free to circumvent a measure protecting rights of a copyright owner in order to make fair use of a work,¹⁵⁰⁹ whereas gaining access in the first instance to a copyrighted work without the

¹⁵⁰⁷ Storage Technology Corp. v. Custom Hardware Eng’g & Consulting, Ltd., 2006 U.S. Dist. LEXIS 43690 at *15, *22 (D. Mass. June 28, 2006).

¹⁵⁰⁸ Id. at *25-26.

¹⁵⁰⁹ See The Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary (Dec. 1998) at 4 (explaining that the distinction between Section 1201(a) and (b) as to the act of circumvention in itself was “to assure that the public will have the continued ability to make fair use of copyrighted works. Since copying may be a fair use under appropriate circumstances, *section 1201* does not prohibit the act of circumventing a technological measure that prevents copying.”). Similarly, the Copyright Office noted in its rationale for the first set of exemptions it established from the prohibition against circumvention of technological measures controlling access to a work: “The decision not to prohibit the conduct of circumventing copy controls was made, in part, because it would penalize some noninfringing conduct such as fair use.” 65 Fed. Reg. 64556, 64557 (Oct. 27, 2000).

owner's permission cannot be a fair use.¹⁵¹⁰ However, many courts have held that fair use does not constitute a defense to anti-circumvention claims under both Sections 1201(a) and 1201(b):

(i) Universal City Studios v. Corley

This case is discussed in Section II.G.1(a)(13)(iii) above, in which the Second Circuit rejected the defendants' argument that Section 1201(c)(1) could and should be read to allow the circumvention of encryption technology when the protected material would be put to fair uses. The court disagreed that Section 1201(c)(1) permitted such a reading. "Instead, it clearly and simply clarifies that the DMCA targets the *circumvention* of digital walls guarding copyrighted material (and trafficking in circumvention tools), but does not concern itself with the *use* of those materials after circumvention has occurred."¹⁵¹¹

(ii) 321 Studios v. Metro Goldwyn Mayer Studios

This case is discussed in Section II.G.1(a)(13)(viii) above, in which the court ruled that legal downstream use of the copyrighted material by customers is not a defense to a software manufacturer's violation of the provisions of § 1201(b)(1).

(iii) Macrovision v. Sima Products Corp.

This case is discussed in II.G.1(a)(13)(xiv) above, in which the court held that although the DMCA provides for a limited "fair use" exception for certain users of copyrighted works under Section 1201 (a)(2)(B), the exception does not apply to manufacturers or traffickers of the devices prohibited by Section 1201(a)(2).

(iv) The Sklyarov/Elcomsoft Case

This case is discussed in Section II.G.1(a)(14)(i) above, in which the court held that nothing within the express language of the anti-circumvention provisions would permit trafficking in devices designed to bypass use restrictions in order to enable a fair use, as opposed to an infringing use.

(v) Eyepartner v. Kor Media Group

This case is discussed in Section II.G.1(a)(1)(viii) above, in which the court held that fair use is not a defense to a claim under Section 1201(a).

¹⁵¹⁰ Realnetworks, Inc. v. DVD Copy Control Ass'n, 641 F. Supp. 2d 913, 942 (N.D. Cal. 2009) ("The prohibition on individual circumvention conduct only applies with respect to access protection technologies (because fair use can never be an affirmative defense to the act of gaining unauthorized access), not to technologies that prevent copying."); Inna Fayenson, "Anti-Circumvention Provisions of The Digital Millennium Copyright Act," *Journal of Internet Law*, Apr. 1999, at 9, 10.

¹⁵¹¹ Universal City Studios, Inc. v. Corley, 273 F.3d 429, 443 (2d Cir. 2001) (emphasis in original).

(vi) Disney Enterprises v. VidAngel

See the discussion of the district court’s decision upon remand in Section II.G.1(a)(1)(xv) above, in which the court held generally that the fair use defense does not apply to circumvention claims under the DMCA, because Section 107 of the copyright statute states that certain uses of a work are not copyright infringement in violation of Sections 106 and 106A, whereas the prohibition of circumvention is in Section 1201.

(vii) Sony Computer Entertainment America v. Divineo

This case is discussed in Section II.G.1(a)(2)(iii) above, in which the court ruled that downstream customers’ lawful or fair use of circumvention devices does not relieve a defendant from liability for trafficking in such devices under the DMCA.

(viii) Dish Network v. SatFTA

This case is discussed in Section II.G.1(a)(2)(x).b above, in which the court held, citing Realnetworks, Inc. v. DVD Copy Control Ass’n¹⁵¹² that, although the DMCA provides for a limited fair use exception for certain end users of copyrighted works, the exception does not apply to manufacturers or traffickers who violate Section 1201(b)(1).

(ix) Dish Network v. Sonicview

This case is discussed in Section II.G.1(a)(2)(x).d above, in which the court held that fair use is not a defense to Section 1201(a) when its requirements are established.

(x) Realnetworks v. DVD Copy Control Association

This case is discussed in Section II.G.1(a)(2)(xi) above, in which the court held that, while the DMCA provides for a limited fair use exception for certain end users of copyrighted works, the exception does not apply to manufacturers or traffickers of the devices prohibited by Section 1201(a)(2). The court observed that, while it may well be fair use for an individual consumer to store a backup copy of a personally-owned DVD on that individual’s computer, the DMCA has nonetheless made it illegal to manufacture or traffic in a device or tool that permits a consumer to make such copies.

(xi) Apple v. Corellium

The defendant Corellium created a product that enabled users to create and interact with virtualized devices by loading firmware from operating systems like iOS, Android and Linux, thereby providing an environment in which technology security researchers could conduct research with features of interest to them. Apple released at least some components of iOS in software files known as “IPSW” files that were available for free download from Apple’s servers.

¹⁵¹² 641 F. Supp. 2d 913 (N.D. Cal. 2009).

A user was not presented with or required to agree to the iOS Software License Agreement or End User License Agreement before downloading an IPSW file. Many parts of the IPSW files were unencrypted, including the kernel, which is the core of the operating system that has complete control over all system resources. To set up a virtual device using the Corellium product, a user could choose from a prepopulated list of iOS versions and iOS devices and the Corellium product would automatically download the associated IPSW file from Apple's servers, or Corellium could also instruct customers on how to manually download IPSW files from Apple's servers and then load or import those files into the Corellium product to create iOS virtual devices. The Corellium product performed some transformations on iOS, as a result of which the software involved in creating the virtual device derived from a combination of Corellium's code and Apple's iOS code.¹⁵¹³

Apple put several security measures in place to protect its devices, including access to the operating system, including the following:

- *Authorization Server*: According to Apple, upon installing iOS on an Apple device such as the iPhone, the device must first communicate with Apple's "authorization server" for approval. The device sends information to Apple about the physical iPhone and the version of iOS the user seeks to install. The authorization server checks this information, and if the information presented passes the check, returns a cryptographic signature known as an "AP Ticket" authorizing installation on the device. The signed AP Ticket is saved to the device and is required to be checked every time the device tries to run iOS. Corellium disagreed, asserting instead that iOS in the public IPSW distribution had no such requirements – instead, this security function was hard-coded into physical iOS devices.
- *Secure Boot Chain*: Secure boot chain is a way that Apple prevents unauthorized code from running on its systems. The process involves an interaction between iOS and software embedded in the physical device. The boot chain is secure because each step must be verified before the next step can proceed.
- *Buddy Program*: When iOS is freshly installed on an Apple device, the Buddy program runs, which helps the user set up iOS on the device. One portion of the program present the End User License Agreement governing that version of iOS to the user on the device. The user must accept the EULA before the user can continue to interact with any other part of iOS.
- *Trust Cache*: The trust cache is a list of trusted applications that Apple has approved for execution on iOS. The trust cache prevents users from installing and operating

¹⁵¹³ Apple Inc. v. Corellium, LLC, 510 F. Supp. 3d 1269, 1275, 1277 & 1281 (S.D. Fla. 2020), aff'd in part on other grounds and remanded, 2023 U.S. App. LEXIS 11225 (11th Cir. 2023).

unapproved applications on iOS. The trust cache prevents the installation of rogue software and ensures that only Apple-verified applications can be run on iOS.

Apple sued Corellium for copyright infringement and unlawful circumvention under Sections 1201(a)(2) and (b)(1). The court granted Corellium summary judgment on the copyright claim, finding that Corellium's use of iOS was a fair use, principally on grounds that the use was highly transformative and the Corellium product did not compete with Apple's sales of iOS devices.¹⁵¹⁴ With respect to its unlawful circumvention claims, Apple argued that, at a minimum, Corellium circumvented its authentication server validation check, secure boot chain, Buddy program, and trust cache. Apple asserted that only after circumventing these measures could the Corellium product run iOS, which was not designed to run on non-Apple hardware. Corellium disagreed that it circumvented Apple's technological measures, arguing instead that the IPSW files were left unencrypted, unprotected, unlocked, and out in the open for the public to access, copy, edit, distribute, perform, and display.¹⁵¹⁵

Corellium asserted that, because the court had concluded its use of iOS was a fair use, such fair use provided a defense to Apple's Section 1201 claims. The court observed that the Federal Circuit had suggested in dicta, but not decided, in the Chamberlain case (discussed in Section II.G.1(a)(15)(ii) above) that fair use could be a defense to a Section 1202 violation and that the Ninth Circuit had declined to decide the issue in the MDY Industries case (discussed in Section II.G.1(a)(2)(vii) above). The court noted, however, that the Second Circuit in the Corley case (discussed in Section II.G.1(a)(16)(i) above), as well as some district court cases within the Ninth Circuit, had ruled that fair use is not a blanket defense to the circumvention provisions of Section 1201. After reviewing these cases, the court decided that, if it were to adopt Corellium's position that fair use is a defense to Apple's Section 1201 claim, that would effectively render Section 1201 meaningless, and so the better reading of the statute is that adopted by the Corley decision.¹⁵¹⁶ "Therefore, Corellium may make fair use of iOS, but it is not absolved of potential liability for allegedly employing circumvention tools to unlawfully access iOS or elements of iOS."¹⁵¹⁷

However, the court ruled that issues of material fact precluded entry of summary judgment on Apple's Section 1201(a) claims. There was a dispute as to whether Apple had copyrights in all of iOS or only portions of iOS and whether iOS was open for public access. The parties also disputed the nature of Apple's technological measures and the applicability of those

¹⁵¹⁴ See id. at 1284-93. On the transformative factor, the court observed that "the Corellium Product makes available significant information about iOS. A user can see running processes, halt execution of the virtual device, amend the kernel, look at lists of files, clone snapshots, among other things – giving great introspection into aspects of iOS and its operation on iOS devices. These tools are useful to security research and testing. The product creates a new, virtual platform for iOS and adds capabilities not available on Apple's iOS devices." Id. at 1287-88.

¹⁵¹⁵ Id. at 1293.

¹⁵¹⁶ Id. at 1293-95.

¹⁵¹⁷ Id. at 1295.

measures to the IPSW files and, by extension, elements of iOS in those files. In addition, Corellium had raised statutory defenses under Sections 1201(f), (g) and (j), which provide exemptions for reverse engineering, security testing and encryption research, and those defenses also raised factual questions that precluded entry of summary judgment.¹⁵¹⁸

(17) Register of Copyrights' Report on Section 1201

In June 2017, the Copyright Office issued a report of the first comprehensive public study on the operation of Section 1201 since its enactment, titled “Section 1201 of Title 17: A Report of the Register of Copyrights.”¹⁵¹⁹ The report addressed a variety of issues raised by stakeholders during the study. The report concluded that the overall structure and scope of Section 201 remained sound, but recommended certain legislative updates, including expanding existing provisions that allow circumvention of technological protection measures for security and encryption research and adding new provisions to allow circumvention for other purposes, such as use of assistive reading technologies and the repair of devices. The report also recommended a statutory amendment to give the Librarian of Congress discretion to authorize third parties to assist the beneficiaries of temporary exemptions granted via the statute’s triennial rulemaking proceeding. In addition, the report identified changes the Copyright Office to could make under the current regulatory framework to streamline the process for renewing exemptions and otherwise improve upon the rulemaking process for greater efficiency and public participation. Those changes were implemented by the Copyright Office in connection with the seventh triennial rulemaking process initiated in 2017.

(b) Integrity of Copyright Management Information

(1) Definition of CMI

The DMCA contains provisions directed to maintaining the integrity of “copyright management information” (CMI), which Section 1202(c) of the DCMA defines to include the following items of information “conveyed” in connection with copies of a work or the performance or display of a work, including in digital form (but specifically excluding any personally identifying information about a user of a work):

- the title and other information identifying the work, including the information set forth on a copyright notice;
- the name and other identifying information about the author or the copyright owner of the work;

¹⁵¹⁸ *Id.* at 1293-94, 1296.

¹⁵¹⁹ The report may be found at <https://www.copyright.gov/policy/1201/section-1201-full-report.pdf>.

- the name and other identifying information about a performer, writer, or director associated with a work, other than a work performed publicly by radio and television broadcast stations;
- terms and conditions for use of the work;
- identifying numbers or symbols referring to such information or links to such information; and
- any other information that the Register of Copyrights may prescribe by regulation.

The statement of Rep. Coble accompanying the original introduction of the provision in S. 2037 corresponding to Section 1202 noted that the term “conveyed” was “used in its broadest sense and is not meant to require any type of transfer, physical or otherwise, of the information. It merely requires that the information be accessible in conjunction with, or appear with, the work being accessed.” Under this definition, CMI could include information that is contained in a link whose address is conveyed with the copyrighted work. Such information could well be a shrinkwrap license, as such license would convey the “terms and conditions for use of the work,” which is one of the express components of the definition of CMI.

(i) Cases Requiring CMI to be Part of a Technological System or Process

a. The IQ Group, Ltd. v. Wiesner Publishing, LLC

The case of The IQ Group, Ltd. v. Wiesner Publishing, LLC¹⁵²⁰ is one of the most thorough opinions to consider the scope of the definition of CMI, although it and the cases that follow its reasoning construe what qualifies as protectable CMI under the DMCA quite a bit more narrowly than the cases discussed in Section II.G.1(b)(1)(ii) below that reject its reasoning or result. There is thus a significant split in authority over the issue of what qualifies as protectable CMI.

The plaintiff IQ Group and the defendant Wiesner Publishing were business competitors who distributed ads by email to insurance agents on behalf of insurance companies. IQ distributed ads for two insurance companies that contained IQ’s graphic logo. The logo functioned as a hyperlink in the ads such that, when clicked, it directed the user to a page of IQ’s website which IQ claimed contained copyright notices. After IQ had distributed the ads for the two insurance companies, the companies hired Wiesner to distribute the same ads via email. Wiesner removed IQ’s logo and hyperlink, added new information so that responses to the ads would go to the insurance companies, and then copied and distributed the ads by email. IQ sued the two insurance companies and Wiesner for, among other things, violation of the CMI

¹⁵²⁰ 409 F. Supp. 2d 587 (D.N.J. 2006).

provisions of the DMCA based on the removal of the logo from the ads. The parties cross moved for summary judgment.¹⁵²¹

The court ruled that the IQ's claim that the logo and hyperlink were within the scope of Section 1202 failed for two reasons. First, as to the logo, IQ's position impermissibly blurred the distinction between trademark law and copyright law. Second, properly interpreted, Section 1202 did not apply to either the logo or the hyperlink.¹⁵²²

With respect to the first reason, the court ruled that protecting a logo, functioning as a service mark, under the CMI provisions would turn the DMCA "into a species of mutant trademark/copyright law, blurring the boundaries between the law of trademarks and that of copyright."¹⁵²³ Specifically, the court was concerned that if every removal or alteration of a logo attached to a copy of a work gave rise to a cause of action under the DMCA, the DMCA would become an extension of, and overlap with, trademark law. There was no evidence that Congress intended such an extreme outcome in enacting the DMCA.¹⁵²⁴

The court then turned to the proper interpretation of the definition of CMI, noting that the interpretation of that definition was a matter of first impression. Although the court noted that the definition, read literally, seemed to apply wherever any author had affixed anything that might refer to his or her name, examination of the legislative history and other extrinsic sources convinced the court that the statute should be subject to a narrowing interpretation.¹⁵²⁵ Citing an article by law professor Julie Cohen¹⁵²⁶ and the legislative history of the WIPO Copyright Treaty that led to enactment of the DMCA to implement it, the court concluded that protected CMI should be limited to components of automated copyright protection or management systems.

Specifically, WIPO was intended to protect CMI as part of a double protection scheme for technical measures – to allow the protection of copyrighted works by the application of technical measures restricting access thereto and protecting copyright rights therein, and to protect the technical measures themselves against those who would crack them by other technologies or machines. Thus, the court found that in the framework of the WIPO treaties, technical measures such as CMI were viewed as components of automated copyright protection systems.¹⁵²⁷ This same understanding of CMI was embodied in the White Paper of the Information Infrastructure Task Force released in September of 1995, which presented a draft of Sections 1201 and 1202, and noted that systems for managing rights in works were being contemplated in the

¹⁵²¹ *Id.* at 589-90.

¹⁵²² *Id.* at 591-92.

¹⁵²³ *Id.* at 592.

¹⁵²⁴ *Id.*

¹⁵²⁵ *Id.* at 593.

¹⁵²⁶ Julie E. Cohen, "Copyright and The Jurisprudence of Self-Help," 13 Berkeley Tech. L.J. 1089 (1998).

¹⁵²⁷ 409 F. Supp. 2d at 593-95.

development of the national information infrastructure to serve the functions of tracking and monitoring uses of copyrighted works as well as licensing of rights and indicating attribution, creation and ownership interests. To implement these rights management functions, the White Paper noted that information would likely be included in an “electronic envelope” containing a digital version of a work to provide information regarding authorship, copyright ownership, date of creation or last modification, and terms and conditions of authorized uses.¹⁵²⁸

From this the court concluded the White Paper demonstrated that the Working Group on Intellectual Property Rights, in drafting Section 1202, “understood this section to protect the integrity of automated copyright management systems functioning within a computer network environment,” and that this interpretation was confirmed by contemporaneous commentary on the draft provision.¹⁵²⁹ Sections 1201 and 1202 underwent no significant revision between drafting in 1995 and enactment in 1998.¹⁵³⁰

The court noted that this interpretation of Section 1202 made sense because it fit Section 1201 with Section 1202, and with chapter 12 of the DMCA as a whole. “Chapter 12, as a whole, appears to protect automated systems which protect and manage copyrights. The systems themselves are protected by § 1201 and the copyright information used in the functioning of the systems is protect in § 1202. ... Section 1202 operates to protect copyright by protecting a key component of some of these technological measures. It should not be construed to cover copyright management performed by people, which is covered by the Copyright Act, as it preceded the DMCA; it should be construed to protect copyright management performed by the technological measures of automated systems.”¹⁵³¹

In sum, the court ruled that “[t]o come within § 1202, the information removed must function as a component of an automated copyright protection or management system.”¹⁵³² The court found no evidence that IQ intended that an automated system would use its logo or hyperlink to manage copyrights, nor that the logo or hyperlink performed such a function. Accordingly, the logo and hyperlink did not fall within the definition of CMI, and the court granted summary judgment for Wiesner on IQ’s CMI claim.¹⁵³³

b. Textile Secrets Int’l, Inc. v. Ya-Ya Brand Inc.

In this case, the plaintiff alleged that fabrics sold by the defendants infringed the plaintiff’s copyright in its “FEATHERS” fabric design. The plaintiff also alleged that the

¹⁵²⁸ Id. at 594-95.

¹⁵²⁹ Id. at 595.

¹⁵³⁰ Id. Although the Senate Report stated that CMI need not be in digital form, the court noted that the Senate Report gave only a vague idea as to what CMI was intended to be, and there was nothing in it to suggest that the Senate Committee understood Section 1202 differently from the Working Group. Id. at 596.

¹⁵³¹ Id. at 597.

¹⁵³² Id.

¹⁵³³ Id. at 597-98.

defendants had violated the CMI provisions of the DMCA by removing the plaintiff's name and the copyright symbol from the selvage (the edge or border of fabric that is intended to be cut off and discarded) of its fabrics, as well as an attached tag stating that the design was a registered work of the plaintiff, and then making copies of the fabrics. The central issue in the case was whether the information on the selvage and the tag constituted CMI.¹⁵³⁴

The defendants urged that, in view of the legislative history of the DMCA, the CMI provisions should be construed to apply only to transactions on the Internet or in the electronic marketplace. The plaintiff argued that a plain reading of the CMI provisions should lead to a conclusion that CMI can be protected on all types of works, in both digital and non-digital form.¹⁵³⁵ After an extensive survey of the history of the CMI provisions of the DMCA, including the White Paper of the National Information Infrastructure Task Force, congressional reports, and the WIPO treaties, the court ruled that the information on the selvage and the tag did not constitute CMI within the purview of the DMCA.¹⁵³⁶ The court found the IQ Group decision, discussed above, influential to its decision, although it chose not to define the scope of CMI as definitively as that case did.¹⁵³⁷ Nevertheless, the court was persuaded by that case that Section 1202 should be "subject to a narrowing interpretation" as follows:

While the Court does not attempt in this decision to define the precise contours of the applicability of § 1202, the Court nevertheless cannot find that the provision was intended to apply to circumstances that have no relation to the Internet, electronic commerce, automated copyright protections or management systems, public registers, or other technological measures or processes as contemplated in the DMCA as a whole. In other words, although the parties do not dispute that the FEATHERS fabric contained [the plaintiff's] copyright information, there are no facts showing that any technological process as contemplated in the DMCA was utilized by plaintiff in placing the copyright information onto the FEATHERS fabric, or that defendants employed any technological process in either their removal of the copyright information from the design or in their alleged distribution of the design. In short, the Court finds that, in light of the legislative

¹⁵³⁴ Textile Secrets Int'l, Inc. v. Ya-Ya Brand Inc., 524 F. Supp. 2d 1184, 1192-93 (C.D. Cal. 2007).

¹⁵³⁵ Id. at 1193-94.

¹⁵³⁶ Id. at 1194-99.

¹⁵³⁷ Id. at 1202 n.17 ("The Court is not attempting to define or specify what types of non-digital works are covered. Rather, under the particular facts of this case – that is, in the absence of any facts demonstrating that a technological process was utilized in connection with either applying the copyright information to the fabric or in removing such information or in subsequently distributing the design – the Court is not persuaded that the copyright information on the FEATHERS fabric warrants coverage by the DMCA.") (emphasis in original) & 1203 n.18 ("Although the Court is persuaded to some extent by the reasoning set forth in the IQ Group decision, the Court does not find it necessary to define the scope of § 1202 as definitively as the IQ Group court did (i.e., that the provision applies only to copyright management information that functions 'as a component of an automated copyright protection or management system').") (quoting IQ Group, 409 F. Supp. 2d at 598).

intent behind the DMCA to facilitate electronic and Internet commerce, the facts of this case do not trigger § 1202.¹⁵³⁸

c. Jacobsen v. Katzer

In this case, the plaintiff was a leading member of the Java Model Railroad Interface (JMRI) Project, an online, open source community that developed model train software and distributed it under the open source Artistic License. The defendants also developed software for model railroad enthusiasts. The plaintiff brought a claim under Section 1201(b), alleging that the JMRI Project Decoder Definition Files distributed by the JMRI and used by the defendants constituted CMI and that by removing some of the information in the files and making copies of the files, the defendants had violated Section 1201(b). The defendants brought a motion to dismiss the claim.¹⁵³⁹

The information in the files that the plaintiff claimed constituted CMI were the author's name, a title, a reference to the license and where to find the license, a copyright notice, and the copyright owner. The plaintiff alleged that he used a software script to automate adding copyright notices and information regarding the license and uploaded the files on the Internet through Source-Forge.net, and that the defendants downloaded the files and removed the names of the authors and copyright holder, title, reference to the license, where to find the license and the copyright notices, and instead, renamed the files and referred to their own copyright notice and named themselves as author and copyright owner. The court denied the motion to dismiss. It cited the IQ Group case's holding that the statute should be construed to protect CMI performed by the technological measures of automated systems, but found that the complaint alleged there had been some technological process engaged to protect the information inserted into the files. Thus, absent further discovery, the court found it inappropriate to dismiss the CMI claim.¹⁵⁴⁰

In a subsequent opinion ruling on cross motions for summary judgment, the court, citing the IQ Group and McClatchey decisions, ruled that the DMCA protects only "CMI performed by the technological measures of automated systems."¹⁵⁴¹ The court found, based on the allegations in the complaint, that there had been some technological process employed to protect the attribution information in the Decoder Definition Text Files. Further, there was no dispute that the defendants had employed a tool to translate the JMRI files to a format for their own use without copying this attribution information. Accordingly, the court granted summary judgment to the plaintiff that the attribution information constituted CMI protected by the DMCA. However because there remained disputed issues of fact regarding the defendants'

¹⁵³⁸ Id. at 1201-02.

¹⁵³⁹ Jacobsen v. Katzer, 609 F. Supp. 2d 925, 928 & 934 (N.D. Cal. 2009).

¹⁵⁴⁰ Id. at 934.

¹⁵⁴¹ Jacobsen v. Katzer, 2009 U.S. Dist. LEXIS 115204 at *20 (N.D. Cal. Dec. 10, 2009).

knowledge and intent, the court denied the plaintiff's motion for summary judgment on liability under the CMI provisions of the DMCA.¹⁵⁴²

d. Silver v. Lavadeira

The plaintiff published certain news reports on her web site and placed her name within the reports. The plaintiff alleged that the defendant copied certain information from her reports and violated Section 1202 by omitting her name from the copied material. The court ruled, based on IQ Group, that CMI is limited to components of technological measures functioning as automated systems, and that the plaintiff's name did not constitute CMI because she had not alleged that an automated technological system was responsible for the inclusion of her name in the news reports.¹⁵⁴³

(ii) Cases Not Requiring CMI to be Part of a Technological System or Process

a. McClatchey v. The Associated Press

The court in McClatchey v. The Associated Press¹⁵⁴⁴ rejected the ruling of the IQ Group court that CMI must function as a component of an automated copyright protection management system in order to be protected by Section 1202 of the DMCA. In the McClatchey case, the plaintiff was the owner of a photograph she took on the morning of Sept. 11, 2001 as she observed United flight 93 crash into a field near her house. The photograph, which the plaintiff titled "End of Serenity," depicted a mushroom cloud caused by the crash, with a red barn and the rolling hills of Pennsylvania in the foreground. The plaintiff alleged that, in the course of an interview with her, a reporter from The Associated Press took a photograph of "End of Serenity" from a binder of materials she showed the reporter, then without authorization distributed the photo on the AP newswire together with an accompanying article written by the reporter.¹⁵⁴⁵

The plaintiff brought a claim for violation of Section 1202 of the DMCA on the ground that she had included title and copyright information on "End of Serenity," which appeared in the photograph of it that the reporter took, but which was cropped out of the version of the photograph distributed by AP. Citing the IQ Group case, AP contended that Section 1202 was not applicable because the plaintiff's copyright notice on her photograph was not "digital." The plaintiff testified in her deposition that she used a computer program called "Advanced Brochures" in a two-step process to print the title, her name, and the copyright notice on all

¹⁵⁴² Id. at *21.

¹⁵⁴³ Report and Recommendation, Silver v. Lavadeira, No. 08 Civ. 6522 (JSR) (DF) at pp. 2-3 (S.D.N.Y. Jan. 7, 2009) (recommendation of magistrate judge), adopted in its entirety by the district court in Silver v. Lavadeira, 2009 U.S. Dist. LEXIS 15491 at *3 (S.D.N.Y. Feb. 26, 2009).

¹⁵⁴⁴ 2007 U.S. Dist. LEXIS 17768 (W.D. Pa. Mar. 9, 2007).

¹⁵⁴⁵ Id. at *3-4.

printouts of her photograph. The court ruled that this technological process was sufficient to come within a digital “copyright management system” as defined in the statute. Moreover, the court noted that Section 1202(c) defines CMI to include “any” of the information set forth in the eight categories enumerated, “including in digital form.” To avoid rendering those terms superfluous, the court held the statute must also protect non-digital information. Accordingly, the court concluded that the statute was applicable to the facts of the case.¹⁵⁴⁶

AP sought summary judgment on the CMI claim on the ground that the metadata accompanying the photograph distributed by AP stated that the photograph was taken by the plaintiff. However, the court noted that the metadata also identified the plaintiff as a “stringer,” from which recipients could have inferred that AP owned the copyright, and that there was no clear statement notifying recipients that the plaintiff owned the copyright to “End of Serenity.” In addition, the court noted a factual dispute concerning whether the reporter had intentionally cropped the copyright notice out of the photograph, as the plaintiff alleged. Accordingly, the court denied AP’s motion for summary judgment.¹⁵⁴⁷

b. Associated Press v. All Headline News Corp.

In this case, the defendant gathered news stories on the Internet, including those of the Associated Press, and prepared them for republication by its customer sites under its own banner, either rewriting the text or copying the stories in full. It instructed its reporters to remove or alter the identification of the AP as author or copyright holder of the articles. AP brought a claim for common law “hot news” misappropriation and for violation of Section 1202. The defendant brought a motion to dismiss the claims, which the court denied. With respect to the CMI claim, the court rejected the IQ Group court’s definition of CMI as limited to copyright management performed by the technological measures of automated systems. The court found that definition to be inconsistent with the text of the statutory definition, which makes no reference to “the technological measures of automated systems.” Accordingly, the court denied the motion to dismiss the CMI claim.¹⁵⁴⁸

c. Fox v. Hildebrand

In this case, the court rejected the Ya Ya Brand and IQ Group cases, ruling that CMI is not limited to notices that are digitally placed on a copyrighted work. The court found that the reference to “including in digital form” in the statutory definition of CMI in Section 1202(c) indicated that the definition was not limited to notices in digital form. Accordingly, the plaintiff’s allegation that the defendant had copied the plaintiff’s architectural drawings, on which the plaintiff had handwritten a copyright notice, and erroneously designated itself as the copyright

¹⁵⁴⁶ Id. at *4-5, * 15.

¹⁵⁴⁷ Id. at *15-17.

¹⁵⁴⁸ Associated Press v. All Headline News Corp., 608 F. Supp. 2d 454, 457 & 461-62 (S.D.N.Y. 2009).

owner on the copied drawings, stated a claim under Section 1202(b) of the DMCA sufficient to survive the defendant's motion to dismiss.¹⁵⁴⁹

d. Faulkner Press v. Class Notes

In this case, the court ruled that the plain language of the DMCA does not limit the definition of CMI to notices that are placed on works through technological processes. However, it granted summary judgment in favor of the defendant with respect to the plaintiff's claims for removal of CMI and addition of false CMI. The plaintiff owned the copyrights in electronic textbooks and film study questions created by a professor at the University of Florida for two wildlife issues courses. The textbooks had CMI printed on the boxes containing the electronic textbooks and within the textbooks' software. The film study questions were alleged to contain CMI by virtue of a watermark that appeared on the questions when viewed at a website maintained for the professor's course.¹⁵⁵⁰

Class Notes hired students to take notes on the professor's class, and the plaintiff alleged that in the course of the note taking, the students viewed copyrighted material taken from the textbooks and film study questions presented by the professor and copied such material into the Class Notes note package. The plaintiff asserted a removal of CMI claim based on the fact that the Class Notes note package did not reproduce the CMI printed on the boxes of the electronic textbooks, and a false CMI claim based on the fact that the note package had the phrase "Einstein's Notes (c)" printed on it.¹⁵⁵¹

The court rejected both claims. With respect to the claim for removal of CMI, the court noted that Class Notes did not "remove" any CMI contained in the textbooks or on the film study questions. Its student note takers simply took notes from the professor's course and those notes were compiled into note packages. An action for removal of CMI requires the information to be removed from a plaintiff's product or work. Here, nothing was removed from the copyrighted works. Instead, information from the professor's courses was allegedly copied into a different form and then incorporated into the note packages. Hence, no CMI was removed from the plaintiff's product or work. With respect to the claim for false CMI, the court noted that the note packages were a different product from the professor's work even if they included materials from the professor's work. No alteration was made to the professor's product or work, so there was no violation of the DMCA by printing "Einstein's Notes (c)" on the note packages. Finally, even if there was illegal alteration of CMI, the court noted that the plaintiff had presented no evidence to show that Class Notes took any such action with intent to aid

¹⁵⁴⁹ Fox v. Hildebrand, 2009 U.S. Dist. LEXIS 60886 at *2, *5-8 (C.D. Cal. July 1, 2009).

¹⁵⁵⁰ Faulkner Press, LLC v. Class Notes, LLC, 2010 U.S. Dist. LEXIS 123935 at *2, *5 & *13-14 (N.D. Fla. Nov. 23, 2010).

¹⁵⁵¹ Id. at *2-4, *14-15.

infringement. Accordingly, the court granted Class Notes summary judgment with respect to the CMI claims.¹⁵⁵²

e. Interplan Architect v. C.L. Thomas

In this case, the plaintiff developed architectural documents for the defendant and supplied them in both physical and electronic form. The plaintiff alleged that the defendant, without permission, supplied copies of those documents to another architectural firm to build additional stores for the plaintiff, and that in the course of doing so, the defendant intentionally removed or altered CMI provided in physical and/or electronic copies of the plaintiff's documents. The plaintiff identified as its CMI the following information contained in the documents: its logo, the store identifier, and scope of document information. The defendant argued in a motion to dismiss that, in order to have a claim under Section 1202, there must be a notice of copyright in the information comprising CMI. The court rejected this argument, noting that Section 1202 defines CMI as "any" of the list of information types in the statute, only one of which is a copyright notice.¹⁵⁵³

The defendant further argued that the plaintiff's Section 1202 claim must fail because it failed to alleged that a technological process was used for placement and/or removal of CMI. The court rejected this argument, noting that Section 1202(c) defines CMI as information connected to copies or phonorecords "including in digital form," which language implies that the statute contemplates applicability to non-digital works as well. And the court did not find the terms of Section 1202 to be sufficiently ambiguous that it needed to resort to legislative history to decide the issue. Accordingly, the court denied the defendant's motion to dismiss the plaintiff's Section 1202 claim.¹⁵⁵⁴

f. Agence France Presse v. Morel

In Agence France Presse v. Morel,¹⁵⁵⁵ photographer Daniel Morel took photos of Port au Prince, Haiti, shortly after an earthquake devastated the city and posted the photos on TwitPic. There were no copyright notices on the images themselves, but Morel's TwitPic page included the attributions "Morel" and "by photomorel" next to the images. A few minutes after Morel posted his photos, Lisandro Suero copied the photos, posted them on his TwitPic page, and tweeted that he had "exclusive photographs of the catastrophe for credit and copyright." Suero did not attribute the photos to Morel. Agence France Presse (AFP) downloaded 13 of Morel's

¹⁵⁵² Id. at *14-16. Accord Jeehoon Park v. Skidmore, Owings & Merrill LLP, 2019 U.S. Dist. LEXIS 171566 at *33-35 (S.D.N.Y. Sept. 30, 2019) (following Faulkner Press, the defendant architect's claiming authorship of 1 World Trade Center building, which the plaintiff claimed infringed his own copyrighted building design, was not a removal of CMI from the plaintiff's work but rather associating the defendant's name with its own separate work that the plaintiff believed was infringing).

¹⁵⁵³ Interplan Architect, Inc. v. C.L. Thomas, Inc., 2009 U.S. Dist. LEXIS 126705 at *3-4, *8-10 (S.D. Tex. Nov. 13, 2009).

¹⁵⁵⁴ Id. at *11-15.

¹⁵⁵⁵ 769 F. Supp. 2d 295 (S.D.N.Y. 2011).

photos from Suero's TwitPic page (not knowing that Suero had copied them from Morel), placed them on an image forum and transmitted them to Getty, an image licensing company. Morel's photos were labeled with the credit line "AFP/Getty/Lisandro Suero," designating AFP and Getty as the licensing agents and Suero as photographer. Getty then licensed Morel's photos to numerous third party news agencies, including CBS and CNN. After learning that the photos did not belong to Suero, AFP issued a wire instruction to change the photographer credit from Suero to Morel. However, Getty continued to sell licenses to charities, relief organizations, and new outlets that variously credited AFP, Suero, or Morel as the photographer.¹⁵⁵⁶

Shortly thereafter, Corbis, which acted as Morel's worldwide licensing agent emailed Getty asserting exclusive rights to Morel's photos. That afternoon, AFP issued a "kill" for 8 images listing Morel as photographer, but the "kill" did not include identical images credited to Suero or images never credited to Morel. Morel and Corbis alleged that AFP and Getty failed to observe or enforce the credit change instruction or the "kill," continued to license and sell Morel's photos, and derived a direct financial benefit as a result. AFP filed a suit, seeking a declaratory judgment that AFP did not infringe Morel's copyrights in certain photos. Morel counterclaimed against AFP and Getty, alleging that they had willfully infringed his copyrights and that AFP and Getty were secondarily liable for the infringement of others and had violated the CMI provisions. AFP moved to dismiss Morel's counterclaims for failure to state a claim.¹⁵⁵⁷

The court rejected the motion to dismiss the CMI claims. The court declined to adopt the definition of CMI in IQ Group as limited to a component of an automated copyright protection or management system. The court was persuaded by the reasoning of decisions rejecting IQ Group and held that the notations "Morel," "daniel morel," and "photomorel" used by Morel in connection with his photos fell within the scope of CMI under the plain language of the statute.¹⁵⁵⁸

After discovery, the parties filed cross-motions for summary judgment. Morel's CMI claims were based on the distribution of his photos credited to Suero and the distribution of his photos credited to Getty and/or AFP. The court denied the motions based on disputed issues of fact. With respect to AFP, the court found that AFP had provided evidence sufficient for a jury to find that its employee obtained the photos only from Suero's Twitter page and was ignorant of Morel at the time the employee downloaded the photos and therefore did not have the requisite state of mind for CMI liability in crediting the photos to Suero. Morel, on the other hand, alleged that AFP had also obtained some of the photos from Morel's Twitter page and that AFP's employee was therefore aware that Morel held the rights to the photos. But even if the factual issue as to source of the photos were resolved in AFP's favor, the court noted other evidence from which a jury could conclude AFP distributed the photos with false, altered, or removed CMI and did so with the requisite intent. For example Morel presented evidence that the photos were credited to, among others, "DANIEL MOREL/AFP/Getty Images," "Lisandro

¹⁵⁵⁶ Id. at 298-300.

¹⁵⁵⁷ Id. at 298, 300-301.

¹⁵⁵⁸ Id. at 305-06.

Suero/AFP/Getty Images,” “Daniel Morel/Agence France-Presse – Getty Images,” and “AFP/Getty Images/Daniel Morel.” Morel contended that distributing the photos with these credits established a violation of the CMI provisions because including “AFP” and “Getty” in the caption provided false and altered CMI about the ownership of the photos. The evidence also suggested that AFP and Getty added their watermarks to the photos, which the court found facially suggestive of an assertion of ownership. And the addition of “AFP” to the caption could potentially induce, enable, facilitate, or conceal AFP’s infringement and the infringements of its subscribers.¹⁵⁵⁹

The court found similar factual issues with respect to Getty. For example, there was evidence that at least one employee of Getty was aware that there remained on Getty’s system copies of the photos that wrongfully credited Suero and to which Getty did not have a valid license. From that evidence, a jury could find Getty knew that the CMI on the images was false and altered, and intent, knowledge, or reasonable grounds to know that continuing to distribute the photos with incorrect CMI would induce, facilitate, enable, or conceal infringement. In sum, the court denied the cross-motions for summary judgment, finding genuine disputes as to at least the source of the photos (whether they were obtained from Morel or Suero); whether and to what extent the captions to the photos conveyed copyright information; and AFP and Getty’s state of mind in distributing the photos.¹⁵⁶⁰

In a subsequent opinion, discussed in Section III.C.6(b)(1)(iii).v below, the court determined that both AFP and Getty were direct infringers for the distribution of unauthorized copies of Morel’s photos and allowed the case to go to a jury on the copyright infringement claims and the CMI claims. In Nov. 2013, a New York federal jury found that both AFP and Getty had willfully infringed Morel’s copyright in the eight photographs, awarded Morel \$275,000 in actual damages, \$28,889.77 total in infringer’s profits, and \$1.2 million in statutory damages; found that AFP and Getty had jointly committed sixteen violations of the CMI provisions of the DMCA for the distribution of false bylines; and awarded Morel an additional \$20,000 for those DMCA violations. Morel elected to receive statutory damages in lieu of actual damages and infringer’s profits, and the court entered judgment in the total amount of \$1,220,000. As discussed in greater detail in Section III.C.6(b)(1)(iii).v below, the defendants’ subsequent motions for JMOL, new trial and/or remittitur were denied, except Getty’s motion for JMOL with respect to Section 1202(b) liability was granted. AFP and Getty remained jointly liable for \$1.2 million in statutory damages, and AFP was held individually liable for \$10,000 of statutory damages under the CMI provisions of the DMCA (one half of the total the jury awarded against AFP and Getty).¹⁵⁶¹

g. Murphy v. Millennium Radio

¹⁵⁵⁹ Agence France Presse v. Morel, 934 F. Supp. 2d 547, 551 & 576-77 (S.D.N.Y. 2013).

¹⁵⁶⁰ Id. at 578.

¹⁵⁶¹ Agence France Presse v. Morel, 2014 U.S. Dist. LEXIS 112436 at *6-7, *10-29 (S.D.N.Y. Aug. 13, 2014).

The case of Murphy v. Millennium Radio Group LLC¹⁵⁶² was the first federal appellate court decision concerning whether CMI is limited to information that is a component of an automated copyright protection or management system. The plaintiff was the copyright owner of a photo. An unknown employee of the defendant scanned the photo from a magazine and posted the resulting electronic copy to the defendant's web site and to another web site. The resulting image, as scanned and posted to the Internet, eliminated the original photo's gutter credit (i.e., a credit placed in the inner margin, or "gutter," of a magazine page, ordinarily printed in a smaller type and running perpendicular to the relevant image on the page) identifying the plaintiff as the author. The plaintiff brought a claim for violation of the CMI provisions of the DMCA.¹⁵⁶³

The district court had agreed with the reasoning of the IQ Group case and held that the photo credits were in no way a component of an automated copyright protection or management systems and therefore did not qualify as CMI protected under the DMCA.¹⁵⁶⁴ On appeal, the Third Circuit reversed. The Third Circuit noted that the statute imposes no explicit requirement that CMI be part of an automated copyright protection or management system, and rejected the defendants' argument that Section 1202's prohibition on removal of CMI must be interpreted in conjunction with Section 1201's focus on technological measures:

[T]o all appearances, § 1201 and § 1202 establish independent causes of action which arise from different conduct on the part of defendants, albeit with similar civil remedies and criminal penalties. It may strike some as more intellectually harmonious to interpret the prohibition of removal of CMI in § 1202 as restricted to the context of § 1201, but nothing in the text of § 1201 actually dictates that it should be taken to limit the meaning of "copyright management information."¹⁵⁶⁵

Turning to the legislative history of the DMCA, the court found that, while it is possible to read the legislative history to support an interpretation of CMI as limited to a component of an automated copyright protection or management system, that history did not provide an extraordinary showing of contrary intentions on the part of Congress that would justify rejecting a straightforward reading of the statutory language. The court there ruled that CMI is not restricted to the context of automated copyright protection or management systems.¹⁵⁶⁶ "Rather, a cause of action under § 1202 of the DMCA potentially lies whenever the types of information listed in § 1202(c)(1)-(8) and 'conveyed in connection with copies .. of a work ... including in digital form' is falsified or removed, regardless of the form in which that information

¹⁵⁶² 650 F.3d 295 (3d Cir. 2011).

¹⁵⁶³ Id. at 299.

¹⁵⁶⁴ Murphy v. Millennium Radio Group LLC, 2010 U.S. Dist. LEXIS 32631 at *2-3, *8-9 (D.N.J. Mar. 31, 2010).

¹⁵⁶⁵ 650 F.3d at 303.

¹⁵⁶⁶ Id. at 305.

is conveyed.”¹⁵⁶⁷ Accordingly, the Third Circuit vacated the district court’s grant of summary judgment in favor of the defendants on the CMI claim.¹⁵⁶⁸

h. William Wade Waller Co. v. Nexstar Broadcasting

This case involved the question whether a watermark logo in the bottom right hand corner of a photo identifying the copyright owner’s web site constituted CMI. The court ruled that, although it was inclined to agree with a broad reading of what may constitute CMI, it did not need to decide the issue because there was no evidence that the defendants had removed the watermark when they posted the plaintiff’s photos on their web site.¹⁵⁶⁹

i. Leveyfilm v. Fox Sports

In this case, the plaintiff owned the copyright in a sports team group photograph that it licensed to be placed on the cover of an album created by a producer on the condition that a credit line identifying Levey as the photographer would accompany the photo. The producer placed on the back of the album a credit line reading “Photography: Don Levey, Don Levey Studio.” The plaintiff alleged that the defendant Chicago Tribune had published the photograph without authorization on its website. The Tribune did not include the credit from the back cover of the album, but instead included the credit line “(Tribune file photo)” under the photograph. The plaintiff brought claims under Section 1202(a), claiming that this credit line constituted false CMI, and under Section 1202(b) for failure to include the “Photography: Don Levey, Don Levey Studio” credit line with the photo on the website. The Tribune moved to dismiss these claims under Rule 12(b)(6).¹⁵⁷⁰

The Tribune argued that the analog notations on the back of the album jacket did not constitute CMI because they were not part of an automated copyright protection system, or connected with digital media or the Internet or electronic commerce. The court rejected this argument, noting that the plain language of the statute does not require any such connection, and that most courts had reached a similar conclusion. The court also rejected the Tribune’s argument that the credit line “Photography: Don Levey, Don Levey Studio” was not CMI because it said nothing about copyright or copyright ownership. The court ruled that the statute’s plain terms do not require that information contain an express reference to copyright or copyright ownership to qualify as CMI. The court further rejected the Tribune’s argument that notations on the back cover of the album jacket were disconnected from the photograph on the front cover of the album and therefore were not protected CMI. The court found it implausible that a viewer of the record album would not understand that the credit line on the back of the album

¹⁵⁶⁷ Id.

¹⁵⁶⁸ Id. at 310.

¹⁵⁶⁹ William Wade Waller Co. v. Nexstar Broadcasting, Inc., 2011 U.S. Dist. LEXIS 72803 at *2, *10-11 (E.D. Ark. July 6, 2011).

¹⁵⁷⁰ Leveyfilm, Inc. v. Fox Sports Interactive Media, 999 F. Sup. 2d 1098, 1099-1100 (N.D. Ill. 2014).

also referred to authorship of the photo on the front cover of the album. The court therefore denied the Tribune’s motion.¹⁵⁷¹

j. Williams v. Roberto Cavalli S.p.A.

The plaintiffs were well known graffiti artists who had created a mural in San Francisco that contained signature elements identifying them as the creators of the mural. The defendants used high resolution photography to obtain images of the mural and placed the images on a collection of *Just Cavalli* clothing. In designing the collection, the defendants rearranged the artists’ signatures, rendering them indiscernible in the collection, and the brand name “Just Cavalli” was superimposed over images of the mural. The plaintiffs claimed the defendants violated Section 1202 by removing and altering their signatures from images of the mural when they were placed onto items in the collection. The defendants filed a motion to dismiss under Rule 12(b)(6).¹⁵⁷²

The defendants contended that the signatures did not constitute CMI because Section 1202 does not protect signatures. The court rejected this argument, finding that the signatures widely identified the artists as authors of the mural and therefore fell within the scope of Section 1202(c)(2). The court further rejected the defendants’ argument that some technological process must have been used in placing or removing the signatures for Section 1202 to apply. The court found that nowhere in Section 1202 does the text limit the definition of CMI to digital information, and Section 1202(c) defines CMI as any information listed in clauses (1) through (8) of Section 1202(c), “including in digital form,” which phrase would be superfluous if information needed to be in digital form for Section 1202 to apply. Accordingly, the court denied the defendants’ motion to dismiss.¹⁵⁷³

k. Bounce Exchange v. Zeus Enterprise

The plaintiff Bounce alleged that it discovered that the defendant, dba Yieldify, was selling software source code that was substantially similar to Bounce’s proprietary code, including software that directly reproduced portions of the code, structure, sequence and organization of Bounce’s software. Bounce further alleged that Yieldify improperly removed all references to and identifications of “Bounce Exchange” from the software’s source code, in violation of Section 1202’s CMI provisions. For example, Bounce claimed that the terms “bounce” and “bouncex” appearing within statements of the source code itself constituted CMI, because they were a shorthand form of the official name of the author of the work:

bouncex.events = ‘mouse-move.bouncex keydown.bouncex DOM-

¹⁵⁷¹ *Id.* at *1101-04.

¹⁵⁷² *Williams v. Roberto Cavalli S.p.A.*, 2015 U.S. Dist. LEXIS 34722 at *14 (C.D. Cal. Feb. 12, 2015).

¹⁵⁷³ *Id.* at *5-10.

```
MouseScroll.bouncex mouse-wheel.bouncex mousedown.bouncex  
touchstart.bouncex touchmove.bouncex';  
  
Bouncex.body.bind(bouncex.events,function()[])
```

In its own source code, Yieldify had replaced the terms “bounce” and “bouncex” with terms referring to Yieldify. For example, the portion of Yieldify’s source code corresponding to the code above read:

```
yel.events = “mousemove.yieldifyx keydown.yieldifyx DOM-MouseScroll.yieldifyx  
mouse-wheel.yieldifyx mousedown.yieldifyx touchstart.yieldifyx touchmove.yieldifyx”;  
  
Yiel.body.bind(yiel.events,function()[])1574
```

Bounce sought to amend its complaint to add CMI claims and Yieldify argued that such amendment should not be permitted as it would be futile since the terms “bounce” and “bouncex” could not qualify as CMI as a matter of law. The court observed that, given that CMI is broadly defined as information conveyed “in connection with” a copyrighted work, forms of CMI may be contained in the body of a work. Accordingly, Bounce’s use of its name within the code conveyed the identifying information in connection with the works for which Bounce sought copyright protection and was therefore CMI. The court noted that its conclusion was particularly appropriate for source code, which is a distinctive type of work in that it is seldom seen by anyone but software developers. Weaving CMI into the text of the source code might therefore be among the most efficient or security-enhancing ways to include CMI with that code. Accordingly, the court held that the terms “bounce” and “bouncex” constituted CMI.¹⁵⁷⁵

The court rejected three arguments by Yieldify against interpreting the statute in this manner. First, Yieldify argued that what Bounce claimed to be CMI was embedded in the source code to such an extent that it had become a portion of the work. Yieldify contended the DMCA demands a clear demarcation between a copyrighted work and any CMI associated with it, and thus if the purported CMI is a portion of the work it cannot be CMI as a matter of law. The court ruled this was a misconstruction of the term “in connection with.” Examples of CMI recited in Section 1202(c), such as a title, author’s name, and terms and conditions, may easily be displayed as a portion of a work.¹⁵⁷⁶

Second, Yieldify argued that the statutory definition of CMI should be subject to a narrowing interpretation limiting CMI to information that is assigned to the work by automated systems. Because the terms in question were not assigned in that manner, Yieldify argued they cannot be CMI. The court “swiftly” dismissed this argument as impossible to square with the

¹⁵⁷⁴ Bounce Exchange, Inc. v. Zeus Enterprise Ltd., 2015 U.S. Dist. LEXIS 165073 at *2, *6 (S.D.N.Y. Dec. 9, 2015).

¹⁵⁷⁵ Id. at *6-7.

¹⁵⁷⁶ Id. at *7-8.

broad language of Section 1202(c), which speaks of “information conveyed in connection with copies of a work,” which information may be conveyed in digital form.¹⁵⁷⁷

Third, Yieldify argued that the terms “bounce” and “bouncex,” as used in Bounce’s source code, were not specific enough to identify Bounce as the code’s author. The court ruled that merely because these terms could be construed to refer to a different entity called “Bounce” or some permutation thereof did not mean that the terms could not qualify as CMI as a matter of law. Section 1202(c) states that CMI may consist of the name of the author of a work, and does not forbid using abbreviations or short-form version of the author’s name. The court held that the terms “bounce” and “bouncex” were sufficiently linked to the plaintiff’s full corporate name to constitute CMI. Accordingly, the court granted Bounce’s motion to amend its complaint to add claims under Section 1202.¹⁵⁷⁸

I. Carter v. Pallante

In this case, the plaintiff had regained rights to a number of copyrighted songs by exercising termination rights and alleged that the defendants were infringing his copyrights and violating Section 1201(a)(1) by continuing to license the songs and providing false CMI to third parties, including false information about the name of the copyright owner, as well as about terms and conditions for use of the work. The defendants moved to dismiss the Section 1201(a)(1) claim, arguing that the DMCA was not intended to apply to circumstances that do not have any relation to the Internet, electronic commerce, automated copyright protection or management systems, public registers, or other technological measures or processes as contemplated by the DMCA as a whole. The court rejected this argument, ruling that the plain text of the statute proscribes falsely identifying the copyright owner of a song in connection with licensing its rights. No connection to the Internet or electronic commerce is necessary. The court also rejected the defendants’ argument that the plaintiff had not adequately alleged that false CMI was conveyed with copies of the work. The court held that the plaintiff had adequately alleged that false CMI was conveyed with copies of the work by way of the licensing agreements he claimed the defendants entered into with third parties. The plaintiff was not required to plead particularized facts as to how, when, and to whom the defendants communicated false information in connection with the purported licensing agreements, nor could he be expected to at the pleading stage, given that any such information was exclusively within the defendants’ knowledge. Accordingly, the court denied the defendants’ motion to dismiss the DMCA claim.¹⁵⁷⁹

m. Preston Wood & Assocs v. RZ Enters. USA

In this case, the plaintiff supplied copyrighted architectural drawings to the defendants, who created and distributed derivative marketing materials from which the plaintiff claimed they

¹⁵⁷⁷ Id. at *8-9.

¹⁵⁷⁸ Id. at *9-10.

¹⁵⁷⁹ Carter v. Pallante, 256 F. Supp. 3d 791, 795, 801 (N.D. Ill. 2017).

removed the plaintiff's CMI in violation of Section 1202(b). The defendants moved for summary judgment, arguing that there was no removal or alteration of the plaintiff's CMI and that they created their derivative marketing materials from scratch. The court noted that there was ample evidence to raise a genuine issue of material fact regarding whether the defendants created their marketing materials from scratch or by using the plaintiff's architectural works from which the defendants had removed or altered the CMI. The defendants also argued that the notices and legends on the plaintiff's architectural works did not qualify as CMI because they had no relation to the Internet or automated copyright management systems. The court rejected this argument, agreeing with other courts that had held that information need not function as part of an automated copyright protection or management system in order to qualify as CMI. The court therefore denied the defendants' motion for summary judgment.¹⁵⁸⁰

n. etrailer Corp. V. TexTrail, Inc.

In this case, the court – citing among other decisions the Associated Press v. All Headline News Corp. decision discussed in Section II.G.1(b)(1)(ii).b above, ruled that the definition of CMI should not be read narrowly (such as limited to technological processes) and therefore covers a physical “sticker” containing a copyright owner's name and logo placed on an object piece that was visible in photos of the object. The plaintiff's allegations that the defendant digitally removed such sticker from the photos using photo editing software were therefore sufficient to state a claim for relief under Section 1202(b), and the court denied the defendant's Rule 12(b)(6) motion to dismiss. The court noted that it found unpersuasive the reasoning set forth in the case of etrailer Corp. v. Automatic Equip. Mfg., discussed in Section II.G.1(b)(1)(iv).g below, which reached a contrary conclusion on the same facts.¹⁵⁸¹

o. Kobi Karp Architecture v. O'Donnell Dannwolf and

Partners

The plaintiff entered into a contract with a third party to design a residential development in Florida, pursuant to which he prepared drawings. Subsequently, the third party hired the defendants to replace the plaintiff as the architect of the project. After taking over the project, the defendants submitted an application to the Miami-Dade County Historic Preservation Board seeking a Special Certificate of Appropriateness for construction of a historical structure on the property. The works that were submitted were slightly altered versions of the plaintiff's copyrighted drawings and bore the plaintiff's registered trademarks. The defendants removed information regarding the plaintiff's authorship before submitting the drawings. The plaintiff asserted claims for copyright infringement and violation of the CMI provisions of the DMCA.¹⁵⁸²

¹⁵⁸⁰ Preston Wood & Assocs., LLC v. RZ Enters. USA, 2018 U.S. Dist. LEXIS 74723 at *2-7 (S.D. Tex. May 3, 2018).

¹⁵⁸¹ etrailer Corp. v. TexTrail, Inc., 2019 U.S. Dist. LEXIS 212304 at *3, *9-11 (E.D. Mo. Dec. 10, 2019).

¹⁵⁸² Kobi Karp Architecture & Interior Design, Inc. v. O'Donnell Dannwolf and Partners Architects, Inc., 2020 U.S. Dist. LEXIS 131909 at *2-3 (S.D. Fla. July 27, 2020).

The defendants moved to dismiss the DMCA claim on the ground that the DMCA applies only to “electronic commerce,” citing decisions finding that Congress intended the DMCA to apply only to the electronic marketplace, and therefore a plaintiff must link the removal of the CMI to the Internet, electronic commerce, or any other purpose for which the DMCA was enacted. The court declined to follow those decisions, instead choosing to follow those courts ruling that the CMI provisions apply to non-technological contexts as well.¹⁵⁸³ Accordingly, the court denied the defendants’ motion to dismiss the CMI claim.¹⁵⁸⁴

p. Sheung Wan Gallery Ltd. v. Kagan

The defendant distributed copies of the plaintiff’s sculptures with a copyright notice in a name other than the plaintiff’s name. Among other claims, the plaintiff brought claims under Section 1202(a) for false CMI. The defendant sought dismissal of the claim on the pleadings. In addition to arguing that the plaintiff had not adequately pled the double scienter requirement (which the court rejected), the defendant argued in a footnote that information like the name of an author of a work is not CMI unless it also functions as part of an automated copyright protection or management system. The court rejected this argument, finding persuasive the numerous courts that have rejected the argument.¹⁵⁸⁵

(iii) Cases Refusing to Decide the Issue

a. Aaberg v. Francesca’s Collections

In this case, the plaintiffs, a group of artists who created enamel pins, sued certain distributors and retailers of enamel pins they accused of sourcing and selling knock-offs of the plaintiffs’ designs with false CMI. The plaintiffs placed each artist’s name or trade name, as well as his or her logo or website, on the pin’s packaging, and in some cases on the pin itself, via a digital and technological process involving computer software and printing machinery. The plaintiffs alleged that employees of the defendants purchased pins from various of plaintiffs’ storefronts and sent them to foreign manufacturers to create the allegedly infringing pins containing new, false CMI. The defendants moved to dismiss the complaint under Rule 12(b)(6).¹⁵⁸⁶

The defendants argued that inclusion of only trade names, logos, web site addresses or social media handles, without the actual name of the copyright owner, did not meet the statutory definition of CMI by virtue of the presence of the conjunctive “and” connecting “the

¹⁵⁸³ Id. at *10-11 (relying on Murphy v. Millennium Radio Group LLC, 650 F.3d 295 (3d Cir. 2001); Roof & Rack Products, Inc. v. GYB Investors, LLC, 2014 U.S. Dist. LEXIS 92333 (S.D. Fla. July 8, 2014); Agence France Presse v. Morel, 769 F. Supp. 2d 295 (S.D.N.Y. 2011); and Landscape Design Workshop, LLC v. Minto Communities, LLC, 2018 U.S. Dist. LEXIS 214697 (S.D. Fla. Dec. 21, 2018)).

¹⁵⁸⁴ Kobi Karp, 2020 U.S. Dist. LEXIS 131990 at *12.

¹⁵⁸⁵ Sheung Wan Gallery Ltd. V. Kagan, 2024 U.S. Dist. LEXIS 10230 at *19 (S.D.N.Y. Jan. 18, 2024).

¹⁵⁸⁶ Aaberg v. Francesca’s Collections, Inc., 2018 U.S. Dist. LEXIS 50778 at *1-6 (S.D.N.Y. Mar. 27, 2018).

name of” to “other identifying information about” in the definition of CMI in Section 1202(c). The court rejected this argument, ruling that collectively, a combination of a trade or brand name, a logo, and a website address is sufficient information to identify the copyright owning plaintiff, citing numerous court decisions that have taken a broad view of what constitutes CMI.¹⁵⁸⁷

Next, the defendants argued that Section 1202 was intended to apply only to circumstances relating to automated copyright protection or management systems or other technological measures or processes as contemplated by the DMCA as a whole. The court noted a split in court decisions on the issue, but observed that this narrow understanding of CMI is likely the minority position now, as myriad other courts adjudicating the scope of the DMCA have not limited it in such a fashion. And the court noted that the text of Sections 1201(a) and (b) do not include words or phrases that would suggest that removal or alteration of CMI, or provision of false CMI, must be accomplished in a specific way.¹⁵⁸⁸

The court noted that a similar divide might be developing between those courts that conclude the DMCA requires a showing that the CMI was removed from the plaintiff’s work itself and those that have allowed a claim to proceed with allegations that CMI was recreated anew. The court decided that it need not decide these questions upon a motion to dismiss, because even if the court were to adopt the narrower view of the DMCA, and require the plaintiffs to have *both* plausibly alleged that the CMI was removed or altered by a technological process *and* that the CMI was removed from the plaintiffs’ actual products, and not just left off of a new creation, dismissal would still not be warranted. The plaintiffs were silent on exactly how the defendants allegedly removed the CMI, pleading only that original pins were sent to foreign manufacturers and when the infringing products returned from the foreign manufacturers the plaintiffs’ CMI had been completely removed. It was therefore reasonable to infer based on the allegations that the foreign manufacturers may have used a technological process to replicate the pins and packaging without the plaintiffs’ CMI, rather than creating the products entirely anew based merely on inspiration from the samples. Consequently, drawing that inference in the plaintiffs’ favor, under either proposed legal standard, the court found that the complaint plausibly alleged a violation of Section 1202.¹⁵⁸⁹

(iv) Other Cases Construing the Definition of CMI

a. Empire Med. Review Servs. V. CompuClaim, Inc.

In this case, the plaintiff Empire Medical Review Services developed the source code for a client’s web site that would enable school districts to submit claims for payment to state Medicaid agencies. To assist in developing the source code, Empire hired an independent contractor. The web site software was object oriented software and the names of each of the

¹⁵⁸⁷ *Id.* at *19-20.

¹⁵⁸⁸ *Id.* at *21-22.

¹⁵⁸⁹ *Id.* at *22-24.

software classes contained the phrase “EmpireMedical.” The consultant subsequently assisted the client to develop a replacement version of the web site software, which he developed using the Empire web site source code as a starting point. In the course of the development, he changed the class names in the source code to remove the phrase “EmpireMedical” in the names and substitute the phrase “CMWeb” in its place. Empire sued the client for copyright infringement and violation of Section 1202(b)(1), arguing that “EmpireMedical” referred to the name of the author of the copyrighted software and therefore constituted CMI. The client sought summary judgment.¹⁵⁹⁰

The client argued that “EmpireMedical” was not CMI for two reasons. First, it alleged that “EmpireMedical” was not even Empire’s name – there was a separate, unrelated Oregon corporation called “Empire Medical.” Second, it argued that the definition of CMI as including “the name of, and other identifying information about, the author of a work,” requires more than just the name of the author; it requires the name of the author *and* “other identifying information” about the author. The court disagreed with this reading of the definition, finding that it would be inconsistent with the policy and history underlying the DMCA whereby Congress sought broad and common sense protection of copyrighted works. The court found the more reasonable reading to be that Section 1202(c)(2) protects both the name and other identifying information about the author, without requiring both to be included in the work. Thus, the statute does not require that the name of the author be supplemented by “other identifying information about” the author before it can be considered to be CMI. Rather, it simply states that, *if* the author’s name is supplemented by such other identifying information about the author, all of it is CMI. The court ruled that a genuine dispute of material fact existed both as to whether the reference to “EmpireMedical” in a class name in the source code was CMI and as to whether the removal was done with the requisite knowledge. Accordingly, the court denied the defendant’s motion for summary judgment on the CMI claim.¹⁵⁹¹

b. Maule v. Anheuser Busch

In this case, the plaintiff owned the copyright in an altered photograph of the Philadelphia skyline in which he inserted images of two buildings that did not exist at the time of the photo and altered the text of a billboard on top of a building in the photo by changing it from “Locust on the Park; Luxury Loft Apartments” to read “Visit Philly Skyline Dot Com,” a web site he owned. The plaintiff sued the defendant for copyright infringement based on a neon sign the defendant created showing a condensed, less detailed rendering of the Philadelphia skyline. The court dismissed that claim for lack of substantial similarity. The plaintiff also asserted that the defendant violated Section 1202(b) by not including his “Visit Philly Skyline Dot Com” language on the neon sign. The court also dismissed this claim, both on the ground that the sign did not infringe the plaintiff’s copyright, and also on the ground that the billboard in the plaintiff’s photo was not CMI. The plaintiff contended that “Visit Philly Skyline Dot Com” was CMI because it served as an announcement to the viewer as to who controlled the photo. The court rejected

¹⁵⁹⁰ Empire Med. Review Servs. v. CompuClaim, Inc., 326 F. Supp. 3d 685, 688-89 & 691 (E.D. Wisc. 2018).

¹⁵⁹¹ Id. at 691-94.

this argument, noting that the billboard text did not contain the plaintiff's name or any identifying information about him as the author of the photo or owner of the copyright to that work, nor did it inform the public that something was copyrighted or prevent infringement. The mere inclusion of the name of an apparent web site in the photo, without more, did not identify the plaintiff as the creator or owner of the photo, and the court therefore dismissed the Section 1202(b) claim.¹⁵⁹²

c. SellPoolSuppliesOnline.com v. Ugly Pools Arizona

In this case, the plaintiff brought a claim for false copyright marking under Section 1202(a). The plaintiff alleged that the defendants copied the plaintiff's copyrighted photos onto the defendants' web site and provided false CMI on the web site with the intent to induce, enable, facilitate, or conceal infringement. The court granted summary judgment to the defendants. It was undisputed that the defendants' copyright notice on their web site was located only at the bottom of the web site and was not placed next to any of the plaintiff's photos, that the defendants did not add their copyright notice to the plaintiff's photos, and that the defendants did not remove or change the plaintiff's copyright marking from any of the plaintiff's photos. The court ruled that the copyright notice at the bottom of the web site was not conveyed in connection with the plaintiff's photos as required by Section 1202(c) because that notice did not appear next to the photos. The defendant's copyright notice was in a shaded block that separated the copyright notice from the content on the web pages, including the photos. Because the copyright notice was not in the body of, or the area around, the photos at issue, it was not conveyed in connection with the photos in a way that made the copyright notice CMI.¹⁵⁹³

On appeal, the Ninth Circuit affirmed. The Ninth Circuit found the district court had correctly determined that the plaintiff's claim for the improper removal of CMI failed because the plaintiff had not shown that the defendants removed any of the plaintiff's CMI. The information allegedly removed did not identify the plaintiff as the owner or author of any content on the website, and the plaintiff admitted that the information was a fictitious name. The fictitious name also did not identify the title of the plaintiff's website, "SPSO Website www.poolsandpartsnow.com." Thus, the information allegedly removed was not the plaintiff's CMI.¹⁵⁹⁴

The Ninth Circuit also ruled the district court properly determined that the plaintiff's false CMI claim failed because the defendants' copyright notice was not conveyed in connection with copies of the plaintiff's work. The district court had properly limited the work that was the subject of the false CMI claim to the plaintiff's photos. The Ninth Circuit found upon de novo

¹⁵⁹² Maule v. Anheuser Busch, LLC, 2018 U.S. Dist. LEXIS 125805 at *2-4, *10-13 & *16-17 (E.D. Pa. July 27, 2018).

¹⁵⁹³ SellPoolSuppliesOnline.com LLC v. Ugly Pools Arizona, Inc., 344 F. Supp. 3d 1075, 1078 & 1083 (D. Ariz. 2018), aff'd, 2020 U.S. App. LEXIS 10348 (9th Cir. Mar. 31, 2020).

¹⁵⁹⁴ SellPoolSuppliesOnline.com LLC v. Ugly Pools Arizona, Inc., 2020 U.S. App. LEXIS 13048 at *3 (9th Cir. Mar. 31, 2020).

review that there was no genuine dispute that the plaintiff's work included only the photos with the "©CMP" marking. The defendant's copyright notice did not meet the definition of CMI because it was not conveyed in connection with the plaintiff's photos. The defendants' copyright notice was located at the bottom of the web page in a shaded box, separating it from the rest of the content on the web page; the defendants' notice was generic and did not communicate that the defendants owned the photos; the defendants' notice was not located on or next to the plaintiff's photos; and the plaintiff's photos were imprinted with their own copyright markings. The Ninth Circuit therefore affirmed.¹⁵⁹⁵

d. Alan Ross Mach. v. Machinio

The plaintiff alleged that the defendant scraped sales listings of industrial machinery from the plaintiff's web site, removed the plaintiff's copyright notices from the listings, and reproduced them on its own web site under its own copyright notices in violation of Sections 1202(a) and (b). The court ruled that the plaintiff's claim for removal of CMI failed because the only potential CMI associated with the listings was a general copyright notice at the bottom of the web site with no indication of what it referred to. The plaintiff did not allege that the listings or the photos or descriptions in the listings contained CMI, which was important because the plaintiff had alleged that the defendant reproduced those photos and descriptions, not the web pages. The plaintiff argued that it was implausible that the copyright notice would not encompass the listings.¹⁵⁹⁶ But the court refused to make such an inference given the plaintiff's allegations that "[e]ach page of [the plaintiff's] website ... display[s] a notice that the *pages* are copyrighted by [the plaintiff]."¹⁵⁹⁷ The court ruled that without allegations by the plaintiff that the defendant removed or altered any CMI from the *listings* it allegedly copied, the plaintiff failed to allege a violation of Section 1202(b).¹⁵⁹⁸

With respect to its claim for distribution of false CMI, the plaintiff alleged that the Terms of Use page on the defendant's site constituted false CMI because it included false representations about the ownership of copyrighted and trademarked material on the web site. The court rejected this claim because general copyright notices are not "conveyed" with the work as required by Section 1202(a). The court supported its conclusion by noting that a reasonable inference from the plaintiff's allegations was that the defendant's Terms of Use were located on a different page from the listings, or at the very least were not located near the duplicated listings. The court therefore granted the defendant's motion to dismiss the CMI claims.¹⁵⁹⁹

¹⁵⁹⁵ Id. at *3-4, *6.

¹⁵⁹⁶ Alan Ross Mach. Corp. v. Machinio Corp., 2018 U.S. Dist. LEXIS 195415 at *2, *5 (N.D. Ill. Nov. 16, 2018).

¹⁵⁹⁷ Id. at *5 (emphasis added).

¹⁵⁹⁸ Id.

¹⁵⁹⁹ Id. at *7-18, *13.

The plaintiff filed a second amended complaint again including claims under Sections 1202(a) and (b), and the defendant again moved to dismiss. The plaintiff alleged that the following items constituted CMI that were removed by the defendant from the listings it copied: a general copyright notice displayed in the footer of every page of the defendant's web site stating "© 2018 – Alan Ross Machinery Corporation," the HTML source code for the footer, and a link in the footer on every page of the web site to the site's terms and conditions. The court granted the defendant's motion to dismiss with prejudice. The court held that a general copyright notice on each web page was not CMI for the individual photos on those pages because not all photos on the web site were owned by the plaintiff. There was nothing to suggest that the notice applied other than to the actual pages of the web site, and the plaintiff had not alleged that the defendant copied the plaintiff's pages, but rather only the photos and descriptions contained in the listings. There was nothing near the photos indicating who owned them. Nor had the plaintiff alleged that CMI contained in the HTML code for the page referred to anything but the pages themselves or the code for how they were laid out, and the defendant had not alleged that those pages and instructions were copied. The court also held that the link to the plaintiff's terms and conditions was not CMI conveyed in connection with the copied works because the terms and conditions were located on a separate page than the listings copied. And the terms and conditions did not even state that the plaintiff owned any of the information contained on its web site – only that visitors were prohibited from copying and distributing content from the site without the plaintiff's consent. Accordingly, the court granted the defendant's motion to dismiss the second amended complaint with prejudice.¹⁶⁰⁰

e. **Mango v. BuzzFeed**

The plaintiff Mango owned a photo that he licensed to the *New York Post* and alleged that BuzzFeed subsequently published a copy of the photo on its web site, BuzzFeed News, without licensing the photo or otherwise obtaining permission. When the *New York Post* used the photo in connection with an article published on its web site about a litigation, the name "Gregory P. Mango" appeared in a "gutter credit" as a separate line of text below the photo but above the article text. When the photo was later downloaded by BuzzFeed from the *New York Post* article, its metadata did not contain any gutter credit or other attribution to Mango, but provided a hyperlink to the *New York Post* article. The day after the lawsuit settled, a BuzzFeed reporter wrote an online article for BuzzFeed covering the lawsuit, in which he included an unlicensed copy of the photo without attribution to Mango. The reporter testified that he did not see the gutter credit at the time he downloaded the photo, which was then published with the BuzzFeed article with a gutter credit listing "Fisher & Taubenfeld," a law firm involved in the litigation. Mango brought a claim under Section 1202(b) for distribution with missing or altered CMI.¹⁶⁰¹

¹⁶⁰⁰ Alan Ross Mach. Corp. v. Machinio Corp., 2019 U.S. Dist. LEXIS 47484 at *1, *4-11 & *13 (N.D. Ill. Mar. 22, 2019).

¹⁶⁰¹ Mango v. BuzzFeed, Inc., 356 F. Supp. 3d 368, 372-73 (S.D.N.Y. 2019).

The court noted that Section 1202(b) has a “double scienter” requirement, and ruled that a violation of the prohibition on distribution with missing or altered CMI requires a showing of four elements: (1) the existence of CMI on the infringed work; (2) distribution of the infringed work containing missing and/or altered CMI; (3) that the distribution was done knowing that the CMI was removed and/or altered without permission; and (4) that the distribution was done knowing that it would induce, enable, facilitate, or conceal an infringement. Applying this test, the court held under prong (1) that gutter credits constitute CMI under the statute, and that in order to be “conveyed” with a copyrighted work, the gutter credit need not be on the photo or present in the photo’s metadata to constitute protected CMI. Prong (2) was satisfied because BuzzFeed distributed the photo on its news web site with the altered gutter credit listing “Fisher & Taubenfeld” without Mango’s permission. With respect to prong (3), the court found that BuzzFeed knew the gutter credit was altered and removed because the BuzzFeed reporter did the alteration himself. The court found his testimony that the gutter credit was hard to see was not credible given his familiarity as an experienced reporter with gutter credits and the training he had received from BuzzFeed concerning the unauthorized use of copyrighted material. With respect to prong (4), the court found, for similar reasons, that BuzzFeed had reason to know distribution with the altered CMI concealed infringement. The reporter testified that he understood from his training and experience that he was required to get permission to use photos. The court therefore concluded that he should have reasonably known that altering the gutter credit to include a false attribution to the Fisher and Taubenfeld law firm would have wrongfully implied that BuzzFeed had permission to use the photo, thus concealing its infringement. The court therefore ruled that BuzzFeed was liable for violation of Section 1202(b) and granted Mango’s request for statutory damages of \$5,000 and an award of attorneys’ fees and costs.¹⁶⁰²

f. Roth v. Walsh Co.

In this case, the plaintiff, a professional photographer, licensed the defendant to use one of his photographs in the defendant’s catalog subject to the condition that the photo be credited to the plaintiff. The plaintiff alleged that the defendant infringed his copyright by reproducing, displaying and distributing the photograph on the defendant’s websites without any attribution to him. He also brought a claim for violation of Section 1202(a)(1) on the ground that the defendant included its own company name or trademarked logo on or directly adjacent to each unauthorized display of the photograph, which constituted false CMI.¹⁶⁰³

The defendant moved to dismiss the Section 1202(a)(1) claim based on Section 1202(c), which excepts from the definition of CMI any personally identifying information about a user of a work or of a copy, phonorecord, performance, or display of a work. The defendant argued that

¹⁶⁰² *Id.* at 377-79. See also Recif Res., LLC v. Juniper Capital Advisors, L.P., 2020 U.S. Dist. LEXIS 175431 at * 25-26 (S.D. Tex. Sept. 24, 2020) (granting summary judgment on a Section 1202(b) claim because deliberate removal of the copyright owner’s logo and replacing it with the defendant’s own logo wrongfully implied that the defendant had permissions to use the copyrighted work, thus concealing its own infringement).

¹⁶⁰³ Roth v. Walsh Co., 2019 U.S. Dist. LEXIS 11439 at *1-4 (E.D. Wis. Jan. 24, 2019).

because the plaintiff's complaint defined the defendant as a "user" of the photograph (i.e., by alleging that the defendant used the photograph for commercial promotion of its equestrian equipment) and because personally identifiable information includes names, the name of a user of a work is not, and cannot, be CMI. The court noted that, in essence, under the defendant's theory, if one takes another's work and places his or her own name on it, because he or she is using personally identifying information about a user of the work, he or she cannot violate Section 1202(a). Thus, under the defendant's rationale, the court noted it would seem Section 1202(a) could be invoked only in the unlikely situation that one provides some *other* false name on another's work rather than his or her own.¹⁶⁰⁴

The court rejected the defendant's theory, because taking it to the extreme, virtually any person who took another's work and placed their name or brand on it could be considered a "user of a work" rather than an infringer and escape liability. The court concluded it cannot be that an alleged infringer can escape liability under Section 1202(a) simply because the false CMI put forth is the alleged infringer's own name. Accordingly, the court held that the plaintiff's complaint alleging that the defendant included its own company name or trademarked log on or directly adjacent to each unauthorized display of the plaintiff's copyrighted photography alleged sufficient facts to indicate the defendant did so knowingly and with the intent to induce, enable, facilitate, or conceal infringement. The plaintiff's complaint therefore properly stated a claim under Section 1202(a), and the motion to dismiss was denied.¹⁶⁰⁵

g. etrailer Corp. v. Automatic Equip. Mfg.

The plaintiff was an online vendor of motor vehicle accessories and owned copyrights in photos and videos of its products that it posted on its web site. The defendant copied, modified and displayed the plaintiff's photos and videos on its web site. The plaintiff placed a stamp with its company name and logo on its physical towing products themselves, which logo then appeared in the photos and videos of those products on its web site. The plaintiff alleged that when the defendant copied the photos onto its web site, the defendant removed or obscured the etrailer logo in violation of Section 1202(b). The defendant moved to dismiss on the ground that the logo did not constitute CMI for the photos and the court agreed:¹⁶⁰⁶

The Court does not understand how stamping the plaintiff's "etrailer" logo on a towing part could reasonably represent notice of a copyright regarding a photograph of that part used to advertise its sale on the plaintiff's website. Stamping "etrailer" on the towing part itself cannot possibly alert anyone to the fact that a photograph of that towing part appearing on the plaintiff's website has been copyrighted. Stamping "etrailer" on the towing part only indicates that etrailer is the seller of the towing part, not that etrailer is

¹⁶⁰⁴ Id. at *6-7.

¹⁶⁰⁵ Id. at *8-9.

¹⁶⁰⁶ etrailer Corp. v. Automatic Equip., Mfg., 2019 U.S. Dist. LEXIS 63873 at *3-4, *9 (D. Neb. Apr. 15, 2019).

the owner of a copyright to all photographic images of every product it sells through its website.¹⁶⁰⁷

The court further reasoned that CMI is intended to inform the public that an image or work is copyrighted and thereby prevent copyright infringement. Stamping products the plaintiff sells on its web site with its logo was intended to inform the public that the plaintiff sold that particular product. The court therefore found the logo not to be the kind of information Section 1202 was intended to protect, and ruled that the plaintiff had thus failed to state a claim for relief for unauthorized removal of CMI.¹⁶⁰⁸

h. Energy Intelligence Grp. v. Kayne Anderson Capital

Advisors

In this case, the plaintiff published a daily newsletter called *Oil Daily* that provided news and analysis about the North American petroleum industry. The defendant purchased a single subscription to *Oil Daily*, but one of its employees shared access to that subscription with several fellow employees and other third parties – initially by sharing his username and password and later by distributing emailed PDF copies of the publication – in violation of the subscription agreement. The plaintiff brought claims for copyright infringement and violation of the CMI provisions of the DMCA.¹⁶⁰⁹

As delivered by the plaintiff, the PDF copies of *Oil Daily* were named in the format “DE” followed by the date in YYMMDD format. Before forwarding the PDF copies to third parties, the employee renamed each PDF file as “123.” The plaintiff brought claims under Sections 1201 and 1202 based on the renaming of the PDF files. The defendant argued that as a matter of law a PDF filename is not CMI because it is not listed in Section 1202(c) and because downloading and renaming files is a common practice in the modern Internet era. The court rejected these arguments, observing that nothing in Section 1202 indicates that a digital file name cannot be CMI. The court found that a PDF’s file name may be CMI if it is conveyed in connection with copies of the underlying work and contains a title and other information identifying the work. The plaintiff presented evidence at trial indicating that the “DE” naming convention was information identifying each *Oil Daily* newsletter. The court therefore concluded that the PDF file names of *Oil Daily* were CMI.¹⁶¹⁰

i. Mills v. Netflix

¹⁶⁰⁷ *Id.* at *10-11.

¹⁶⁰⁸ *Id.* at *11.

¹⁶⁰⁹ *Energy Intelligence Grp., Inc. v. Kayne Anderson Capital Advisors, L.P.*, 948 F.3d 261, 264-67 (5th Cir. 2020).

¹⁶¹⁰ *Id.* at 267, 277. At trial, the plaintiff presented evidence that the defendant’s employees believed that by renaming the *Oil Daily* newsletters “123,” they would be able to avoid detection of illicit sharing. *Id.* at 277 n.16. The jury found 425 alterations of the file names and imposed statutory damages of \$2,500 for each alteration. *Id.* at 275.

The plaintiff Austin Mills brought copyright infringement claims against the defendants' alleged unauthorized use of clips from the plaintiff's copyrighted YouTube video titled "Fyre Festival COMPLETE Disaster. VLOG of Chaos!" in the defendants' documentary film released on Netflix. The plaintiff asserted claims under Sections 1202(a) and (b). The court granted a motion to dismiss those claims for failure to state in the complaint any factual basis for any of the allegations made on information and belief to support the Section 1202 claims. First, the court noted that the clips from the YouTube video contained in the documentary included the plaintiff's name ("@AUSTINJMILLS") on the bottom left corner, and the plaintiff's name was listed under the category "Additional Archival materials by" in the documentary's credits. The court ruled that the inclusion of the plaintiff's name as the source of the clips demonstrated the plaintiff's conclusory allegations upon information and belief that the defendants knew and intended to induce infringement by altering CMI with respect to the plaintiff's name in the documentary were not plausible. Therefore, the plaintiff had failed to plead sufficient facts regarding the defendants' knowledge and intent as required for his Section 1202 claim.¹⁶¹¹

Second, the court noted that the Section 1202 claim was also based in part on the defendants' alleged removal of the title "Fyre Festival COMPLETE Disaster. VLOG of Chaos!" from the plaintiff's YouTube video. The court observed that other courts have interpreted Section 1202 to require that CMI be removed or altered from the body of or the actual work itself. Here, the title "Fyre Festival COMPLETE Disaster. VLOG of Chaos!" did not appear on the plaintiff's YouTube video. Rather, the title was written on the web site where the plaintiff's video was posted. However, the plaintiff's Section 1202 claim was based on the defendants' alleged infringement of the YouTube video itself, not the web site where the video was posted. Accordingly, the court ruled that the plaintiff's Section 1202 claims failed as a matter of law to the extent it was based on the defendants' alleged removal of the title "Fyre Festival COMPLETE Disaster. VLOG of Chaos!" from the plaintiff's YouTube video.¹⁶¹²

j. Hong v. Recreational Equipment

Hong was an artist who created an illustration titled "Tree Rings," depicting the inner-tree rings of a tree trunk. He alleged that the defendant affixed a version of his "Tree Rings" to two specialty climbing bags and put false CMI on the bags in the form of bag titles "Krieg Tree Rings Green Chalk Bag" and "Krieg Special K Chalk Bag – Bigfoot," thereby making it appear that the defendant was the true owner of "Tree Rings." The defendant moved to dismiss the false CMI claim on the ground that the titles of the bags are not CMI. The court rejected this argument and ruled that Hong had stated a plausible claim under Section 1202(a) because the brand name "Krieg" was included within the name of each of the allegedly infringing bags. And on the defendant's web site pages, the name of each bag appeared directly to the side of the image of the applicable bag. Also included on each bag was a Krieg logo tag next to the "Tree

¹⁶¹¹ Mills v. Netflix, Inc., 2020 U.S. Dist. LEXIS 17797 at *1-2, *7-8 (C.D. Cal. Feb. 23, 2020).

¹⁶¹² Id. at *8-9.

Rings” work on the bag. These court ruled that these allegations were sufficient to avoid the defendant’s motion to dismiss.¹⁶¹³

k. Advanta-Star Auto. Research v. Reynolds Ford

The plaintiff owned copyrights to certain automobile reviews and other automobile-related information that it sold or licensed to dealerships for educational and sales purposes. The plaintiff alleged that the defendant placed the plaintiff’s content on its web pages after intentionally modifying the content to conceal its source, in violation of Section 1202(a). The defendant moved to dismiss the claim on the ground that its copyright notice, which was located at the bottom of its web pages, did not qualify as CMI because the notice was not “conveyed in connection with” the allegedly infringed content since it was located in a generic web site footer rather than near or next to the allegedly infringed content. The court rejected this argument, distinguishing other cases holding that copyright information in a generic footer at the bottom of a web page is not information conveyed in connection with the copyrighted material. Here, the alleged copyrighted work was in fact the text comprising the body of the web pages, so the notice in the footer could constitute CMI. Accordingly, the court ruled that the plaintiff’s Section 1202(a) claim had been adequately pled.¹⁶¹⁴

l. Yellow Pages Photos v. Dex Media

The defendant owned a compilation copyright in a yellow pages directory that included some of the plaintiff’s photos both on the cover of the directory and in some of the advertisements inside the directory. The plaintiff brought a claim under Section 1202, arguing that the defendant’s copyright notice in its name in the bottom right corner of the cover page of its directory constituted a false copyright notice as to the plaintiff’s photos in the directory. The court noted that no previous court had addressed the issue whether a copyright notice on the cover of a publication conveys CMI about individual components of that publication such as copyrighted or copyrightable pictures or images contained therein.¹⁶¹⁵

The court concluded that, as a matter of law, the defendant’s copyright notice did not constitute CMI as to any of the plaintiff’s photos appearing either on the cover (despite the fact that the plaintiff’s photo was displayed on the cover right above the defendant’s copyright notice) or inside the directory. The copyright notice for the directory did not appear on the subsequent pages of the directory or on any images or photos that were used in advertisements in the directory. The copyright notice did not contain any indication that it was associated with or linked to any of the plaintiff’s photos. The directory was a compilation in which the defendant

¹⁶¹³ Hong v. Recreational Equipment, Inc., 2020 U.S. Dist. LEXIS 131393 at *1-2, *8-10 (D. Ida. July 23, 2020).

¹⁶¹⁴ Advanta-Star Auto. Research Corp. v. Reynolds Ford, Inc., 2020 U.S. Dist. LEXIS180538 at *1-2, *9-11 (W.D. Okla. Sept. 30, 2020).

¹⁶¹⁵ Yellow Pages Photos, Inc. v. Dex Media, Inc., 2021 U.S. Dist. LEXIS 42188 at *7, *12-14 (M.D. Fla. Feb. 3, 2021).

had a separate copyright and the defendant was thus entitled to convey CMI about its own work. The court therefore granted summary judgment to the defendant.¹⁶¹⁶

(2) Prohibitions on False CMI and Removal/Alteration of CMI

Section 1202(a) prohibits any person from knowingly providing CMI that is false or distributing or importing for public distribution CMI that is false, with the intent to induce, enable, facilitate, or conceal infringement. Section 1202(b) prohibits any person from intentionally removing or altering any CMI, distributing or importing for distribution CMI knowing that it has been altered or removed, or distributing, importing for distribution, or publicly performing works in which CMI has been removed or altered, in all cases knowing, or, with respect to civil remedies under Section 1203, having reasonable grounds to know, that it will induce, enable, facilitate, or conceal infringement.

(i) Cases re Removal or Alteration of CMI

a. Kelly v. Arriba Soft Corp.

The first case under the CMI provisions was Kelly v. Arriba Soft Corp.¹⁶¹⁷ In that case, the defendant was the operator of a “visual search engine” on the Internet that allowed users to search for and retrieve images. In response to a search query, the search engine produced a list of reduced, “thumbnail” pictures. By clicking on the desired thumbnail, a user could view an “image attributes” window displaying the full-size version of the image, a description of its dimensions, and an address for the website where it originated. By clicking on the address, the user could link to the originating website for the image.¹⁶¹⁸

The search engine maintained an indexed database of approximately two million thumbnail images obtained through the operation of a web crawler that traveled the Web in search of images to be converted into thumbnails and added to the index. The defendant’s employees conducted a final screening to rank the most relevant thumbnails and eliminate inappropriate images. The plaintiff was the owner of the copyright in about 35 photographs that were indexed by the crawler and put in the defendant’s database. The plaintiff sued the defendant for copyright infringement, alleging that storage of the images in the database constituted a direct infringement, as well as a violation of the CMI provisions of the DMCA.¹⁶¹⁹ The court ruled that the defendant’s use of the images in thumbnail form constituted a fair use, and that there was no violation of the CMI provisions of the DMCA.¹⁶²⁰

¹⁶¹⁶ Id. at *22-24.

¹⁶¹⁷ 53 U.S.P.Q.2d 1361 (C.D. Cal. 1999), aff’d in part and rev’d in part on other grounds, 336 F.3d 811 (9th Cir. 2003).

¹⁶¹⁸ Id. at 1362.

¹⁶¹⁹ Id.

¹⁶²⁰ Id. at 1363-67.

The plaintiff argued that the defendant violated the CMI provisions of the DMCA by displaying thumbnails of the plaintiff's images without displaying the corresponding CMI consisting of standard copyright notices in the surrounding text accompanying the photographs on the plaintiff's website from which the crawler obtained the photographs. Because these notices did not appear in the images themselves, the crawler did not include them when it indexed the images. As a result, the images appeared in the defendant's index without the CMI, and any users retrieving the images through the search engine would not see the CMI.¹⁶²¹

The court rejected this claim, holding that Section 1202(b)(1) (which prohibits intentionally removing or altering CMI) "applies only to the removal of copyright management information on a plaintiff's product or original work."¹⁶²² The court also ruled that even if Section 1202(b)(1) did apply, the plaintiff had not offered any evidence showing that the defendant's actions were intentional, rather than merely an unintended side effect of the crawler's operation.¹⁶²³ The court found that the more applicable provision was that of Section 1202(b)(3), which prohibits distribution of copies of works knowing that CMI has been removed or altered without authority of the copyright owner or the law, knowing or having reason to know that it will induce, enable, facilitate, or conceal an infringement. The court also found no violation of this section, however, because users who clicked on the thumbnail version of the images were given a full-sized version, together with the name of the website from which the image was obtained (and an opportunity to link there), where any associated CMI would be available.¹⁶²⁴ "Users were also informed on Defendant's Web site that use restrictions and copyright limitations may apply to images retrieved by Defendant's search engine."¹⁶²⁵ Based on these facts, the court concluded that the defendant did not have "reasonable grounds to know" under Section 1202(b)(3) that it would cause its users to infringe the plaintiff's copyrights:

Plaintiff's images are vulnerable to copyright infringement because they are displayed on Web sites. Plaintiff has not shown users of Defendant's site were any more likely to infringe his copyrights, any of these users did infringe, or Defendant should reasonably have expected infringement.¹⁶²⁶

Accordingly, the court concluded that there had been no violation of the DMCA.

b. Thron v. Harper Collins Publishers

¹⁶²¹ Id. at 1366.

¹⁶²² Id.

¹⁶²³ Id.

¹⁶²⁴ Id.

¹⁶²⁵ Id.

¹⁶²⁶ Id. at 1367.

In Thron v. Harper Collins Publishers,¹⁶²⁷ the plaintiff alleged that the defendant misappropriated two of his allegedly copyrighted photographs for use in a book published by the defendant. The plaintiff further contended that the defendant's subsequent efforts to publicize the book through the Internet violated the CMI provisions of the DMCA because the plaintiff had provided Amazon.com with a digital image of one of the photographs that was allegedly impermissibly altered to remove certain unspecified information related to the plaintiff's copyright registration. The court rejected this claim because the plaintiff's copyright registration was itself invalid and because the plaintiff had submitted no competent, admissible evidence to support any finding that the defendant removed or altered the information intentionally, as required by the statute.

c. Gordon v. Nextel Communications

In Gordon v. Nextel Communications,¹⁶²⁸ the plaintiff brought suit against Nextel and its advertising agency for copyright infringement for the unauthorized use of several of his dental illustrations in a television commercial for Nextel's two-way text message. The plaintiff also claimed a violation of the CMI provisions of the DMCA based on alleged removal of the copyright notice from the illustrations. The district court granted summary judgment on the CMI claims on the ground that the plaintiff failed to present any evidence that the defendants intentionally removed or altered the copyright information or that the defendants knew that the copyright information had been removed.¹⁶²⁹

On appeal, the Sixth Circuit affirmed. The decision is important because the Sixth Circuit ruled for the first time that vicarious liability may apply with respect to violations of the CMI provisions (the rationale of the holding would presumably also apply to the anti-circumvention provisions of the DMCA). In particular, the court held that, regardless of the defendants' actual knowledge of the removal or alteration of the copyright information, they could be held vicariously liable if, just as in the case of ordinary infringement, they had the right and ability to supervise the conduct constituting the violation and they had an obvious and direct financial interest in the conduct.¹⁶³⁰

The court noted that, although the record was not clear in this regard, it was reasonable to infer that the advertising agency retained the ability to supervise the development of the commercial. And both defendants had direct financial interests in the exploitation of the copyrighted materials. As a result, the court ruled that, even though the CMI provisions require the intentional removal of CMI or the distribution of copies of works "knowing" that CMI has been removed or altered, "it is inappropriate to permit summary judgment to be granted based on the defendants' lack of actual knowledge of the removal of the copyright management

¹⁶²⁷ 64 U.S.P.Q.2d 1221 (S.D.N.Y. 2002).

¹⁶²⁸ 68 U.S.P.Q.2d 1369 (6th Cir. 2003).

¹⁶²⁹ *Id.* at 1370.

¹⁶³⁰ *Id.* at 1371.

information when they may be vicariously liable for its removal.”¹⁶³¹ Thus, although the plaintiff had to prove that the direct violators of the CMI provisions possessed actual knowledge of the unauthorized change to the CMI, the plaintiff need not prove that Nextel and its advertising agency, as vicarious infringers, had such knowledge.

Ultimately, however, the Sixth Circuit affirmed the district court’s grant of summary judgment to the defendants on the ground that, even if the persons from whom the advertising agency had obtained the material containing the illustrations upon which the commercial was based had removed the copyright information from the illustrations, those persons testified without contradiction that they believed the materials had been authorized for use in television commercials. Accordingly, such removal was not done with reasonable grounds to know that it would “induce, enable, facilitate, or conceal an infringement,” as required by Section 1202(b).¹⁶³²

d. Monotype Imaging, Inc. v. Bitstream Inc.

In Monotype Imaging, Inc. v. Bitstream Inc.,¹⁶³³ the court adopted a rather broad reading of the scope of the CMI provisions. The plaintiff Monotype developed and distributed fonts and font software. The defendant Bitstream competed with Monotype, and developed a product called TrueDoc, a computer program that facilitated the display of typeface designs on computer screens and other output devices. Bitstream openly promoted the fact that TrueDoc replicated the original typefaces of other vendors. TrueDoc included a Character Shape Recorder (CSR) component that created a compact file format called a Portable Font Resource (PFR) based on an underlying font software program. The CSR obtained data that described the shape of the typeface characters of the underlying font program from the computer’s operating system. When accessing information from the operating system about the font software, TrueDoc did not request the copyright notice from the Windows operating system.¹⁶³⁴ Monotype brought a claim for copyright infringement, apparently based on alleged copying of Monotype’s font software in the course of creating PFR’s that would work with TrueDoc, as well as a claim for violation of the CMI provisions. Bitstream moved for summary judgment.

Monotype claimed that TrueDoc’s failure to copy the copyright notice from its font software programs violated the CMI provisions of the DMCA because it was virtually identical to removing the copyright notice. The court agreed with Monotype that the plain language of the DMCA does not require that TrueDoc, itself, physically remove the copyright notices from the Monotype font software in creating the PFR files. Thus, the court ruled that the mere fact that

¹⁶³¹ Id. at 1372.

¹⁶³² Id. at 1373.

¹⁶³³ 2005 U.S. Dist. LEXIS 7410 (N.D. Ill. Apr. 21, 2005).

¹⁶³⁴ Id. at *2-3.

TrueDoc did not “remove” the copyright notices, but instead made copies of the font software without including the copyright notice, did not preclude liability under the DMCA.¹⁶³⁵

Bitstream argued that there should be no finding of a CMI violation because when TrueDoc retrieved information from the operating system about a font software program, the operating system did not provide the copyright strings. Monotype countered by pointing to the fact that the copyright information is accessible through the operating system, and Bitstream simply chose not to include the copyright notice. Monotype’s expert had examined Bitstream’s TrueDoc source code and opined that Bitstream was capable of engineering TrueDoc to retrieve the copyright notice along with the font software information. The court ruled that, viewing this evidence in the light most favorable to Monotype, the expert testimony created a triable issue of fact whether Bitstream copied Monotype’s fonts without the copyright notices in violation of the DMCA. Accordingly, the court denied Bitstream’s motion for summary judgment on the CMI claim.¹⁶³⁶

Three months later, after a bench trial, the court issued a second opinion ruling that Bitstream was not liable for either copyright infringement or CMI violations.¹⁶³⁷ With respect to CMI, because the court found the plaintiffs had failed to prove that Bitstream’s licensees had used the CSR with any of the plaintiff’s fonts, they had therefore failed to show that Bitstream intentionally removed CMI, or distributed copies of works knowing that CMI had been removed, with knowledge or having reasonable grounds to know that it would induce, enable, facilitate or conceal infringement, as required by Sections 1202(b)(1) and 1201(b)(3) of the DMCA.¹⁶³⁸

The court also found no liability for contributory infringement, again because the plaintiffs failed to prove any direct infringement by Bitstream’s licensees – in particular, that a Bitstream licensee had ever used the CSR to copy the plaintiffs’ fonts.¹⁶³⁹ The court also found the plaintiffs did not present any evidence that Bitstream ever knew that its licensees were using TrueDoc’s CSR with the plaintiffs’ fonts.¹⁶⁴⁰ Citing the Supreme Court’s *Grokster* case, however, the court noted that “a court may impute culpable intent as a matter of law from the characteristics or uses of an accused product.”¹⁶⁴¹ In determining whether the alleged contributory infringer acted with such culpable intent, the court, apparently not believing that the *Grokster* case repudiated any of the *Aimster* case’s holding or rationale, noted that the Seventh Circuit considers the following factors under the *Aimster* case: “(1) the respective

¹⁶³⁵ Id. at *26-27.

¹⁶³⁶ Id. at *27-28.

¹⁶³⁷ Monotype Imaging, Inc. v. Bitstream Inc., 376 F. Supp. 2d 877 (N.D. Ill. 2005).

¹⁶³⁸ Id. at 893.

¹⁶³⁹ Id. at 884.

¹⁶⁴⁰ Id. at 887.

¹⁶⁴¹ Id.

magnitudes of infringing and noninfringing uses; (2) whether the defendant encouraged the infringing uses; and (3) efforts made by the defendant to eliminate or reduce infringing uses.”¹⁶⁴²

The court found that the plaintiffs had not satisfied any of the factors. The plaintiffs had not submitted any evidence to tie the ratio of Bitstream fonts to non-Bitstream fonts available in the marketplace to the proportion of such fonts that Bitstream’s customers actually used with the CSR. Nor had they presented any evidence that Bitstream knew of or encouraged the allegedly infringing uses of TrueDoc. With respect to the third factor, the court noted that Bitstream had made at least some efforts to reduce the risk of infringement of third parties’ intellectual property through the use of TrueDoc, in the form of a “doc-lock” feature with the capability of preventing a third party from using a PFR that it had received for any purpose other than viewing the document with which the PFR came. Bitstream also engineered TrueDoc to honor the embedding flags that font foundries include in their font data, which prohibit a third party from embedding that font into another technology.¹⁶⁴³ Finally, the court found no liability under the inducement doctrine of the Grokster case, because there was no evidence that Bitstream had knowledge of its customers’ alleged infringements, much less that it acted with the “purposeful, culpable expression and conduct” required under the Grokster decision.¹⁶⁴⁴

e. Keogh v. Big Lots Corp.

In Keogh v. Big Lots Corp.,¹⁶⁴⁵ the court ruled that the prohibition of Section 1202(b)(3) of the DMCA against distributing works knowing that CMI has been removed or altered without authority of the copyright owner requires actual knowledge that CMI has been removed. Constructive knowledge of removal of CMI is not sufficient. Once CMI is removed from a work, however, the defendant is required to have only “reasonable grounds to know” (a constructive knowledge standard) that its actions would induce, enable, facilitate, or conceal an infringement of any right under the DMCA. Because the plaintiff had not alleged that the defendant had actual knowledge that CMI had been removed from imported birdhouses having designs that allegedly infringed the plaintiff’s birdhouses, the court granted the defendant’s motion to dismiss the CMI claim under Rule 12(b)(6).¹⁶⁴⁶

f. Goldman v. Healthcare Management Systems

In Goldman v. Healthcare Management Systems,¹⁶⁴⁷ the plaintiff alleged that the defendant had been infringing upon its copyright in a computer program since the plaintiff downloaded the program onto the defendant’s computer, and that the defendant had violated

¹⁶⁴² Id.

¹⁶⁴³ Id. at 887-88.

¹⁶⁴⁴ Id. at 888-89.

¹⁶⁴⁵ 2006 WL 1129375 (M. D. Tenn. Apr. 27, 2006).

¹⁶⁴⁶ Id. at *2.

¹⁶⁴⁷ 2006 U.S. Dist. LEXIS 89009 (W.D. Mich. Dec. 8, 2006).

the CMI provisions of the DMCA by knowingly removing the plaintiff's CMI (apparently in the form of a copyright notice). The court denied the plaintiff's motion for summary judgment, finding numerous disputed facts, including whether the appropriate copyright notices were on the original materials given to the defendant.¹⁶⁴⁸

g. Thomas M Gilbert Architects v. Accent Builders

In Thomas M. Gilbert Architects, P.C. v. Accent Builders & Developers, LLC,¹⁶⁴⁹ the court granted summary judgment in favor of the defendant on a claim under Section 1202(b) for removal of a copyright notice from the plaintiff's architectural plans. The court found no evidence to show that the defendant intentionally removed the notice, or that he had reason to know that its removal would induce, enable, facilitate, or conceal infringement. The defendant testified that he was unfamiliar with copyright law and did not recall seeing the copyright notice when he modified the plaintiff's plans. Accordingly, because the plaintiff had made no showing of the required intent, the court granted summary judgment in the defendant's favor.¹⁶⁵⁰

h. Banxcorp v. Costco

In Banxcorp v. Costco Wholesale Corp.,¹⁶⁵¹ the plaintiff published market research performance indices based on selected banking, mortgage and loan data that were used as benchmarks to measure the rates and performance of the U.S. banking and mortgage markets. Costco entered into an agreement with the defendant Capital One Financial Corp. to provide a co-branded direct banking service. The plaintiff and Capital One entered into a license agreement permitting Capital One to access and use the indices and the data contained therein. The plaintiff alleged that Capital One breached the license agreement by redistributing the indices to Costco in order to benefit the co-branded banking services. The plaintiff asserted a DMCA claim based on allegations that when the defendants copied the indices they altered or removed the CMI that the plaintiff had associated with the data.¹⁶⁵² Specifically, the plaintiff had associated MCI with the indices that read: "(C) [year of publication] BanxCorp. All Rights Reserved." The plaintiff included in its complaint an example of an ad the defendants ran in conjunction with the indices that included the following differing CMI: "National Average of [Annual Percentage Yields] for money market accounts as published by BanxQuote.com as of 5/22/07."¹⁶⁵³

The court held that these allegations were sufficient to survive a motion to dismiss the plaintiff's CMI claim. "At summary judgment, Defendants will have an opportunity to present

¹⁶⁴⁸ Id. at *3-4.

¹⁶⁴⁹ 629 F. Supp. 2d 526 (E.D. Va. 2008).

¹⁶⁵⁰ Id. at 537.

¹⁶⁵¹ 723 F. Supp. 2d 596 (S.D.N.Y. 2010).

¹⁶⁵² Id. at 599-600.

¹⁶⁵³ Id. at 610.

evidence that the placement of the CMI either indicated that it did not refer to the BanxQuote Indices, or was sufficiently removed to demonstrate that Defendants lacked the intent required to show a violation of the DMCA. However, the Court declines to hold that, as a matter of law, CMI must be placed on the actual information on a website in order to state a claim under the DMCA.”¹⁶⁵⁴

i. Agence France Presse v. Morel

The facts of this case are set forth in Section II.G.1(b)(1)(ii) above. In ruling on the motion of Agence France Presse (AFP) to dismiss the claim against it for removal of CMI, AFP argued that CMI must be removed from the photograph itself to state a claim for removal or alteration of CMI. The court rejected this argument, noting that the DMCA defines CMI as information “conveyed in connection with copies” and so does not require the CMI to appear on the work itself. The court found it implausible that a viewer of Morel’s photos would not understand the designations “Morel” and “by photomorel” appearing next to the images to refer to his authorship. While the location of CMI could go to AFP’s intent, that fact issue could not be resolved on a motion to dismiss. As to intent and knowledge of infringement, Morel had alleged that AFP, CNN, and CBS representatives contacted him about his photos, copied them without his permission, and distributed them with altered CMI. He also alleged that, in disregard of the credit change instruction, Getty continued to distribute photos crediting Suero or AFP as photographer. The court concluded that these allegations were sufficient to survive a motion to dismiss.¹⁶⁵⁵

After discovery, the parties cross-moved for summary judgment on the CMI claims. The court denied the motions based on various factual disputes,¹⁶⁵⁶ for the reasons summarized in Section II.G.1(b)(1)(ii).e above. In a subsequent opinion, discussed in Section III.C.6(b)(1)(iii).v below, the court determined that both AFP and Getty were direct infringers for the distribution of unauthorized copies of Morel’s photos and allowed the case to go to a jury on the copyright infringement claims and the CMI claims. In Nov. 2013, a New York federal jury found that both AFP and Getty had willfully infringed Morel’s copyright in the eight photographs, awarded Morel \$275,000 in actual damages, \$28,889.77 total in infringer’s profits, and \$1.2 million in statutory damages; found that AFP and Getty had jointly committed sixteen violations of the CMI provisions of the DMCA for the distribution of false bylines; and awarded Morel an additional \$20,000 for those DMCA violations. Morel elected to receive statutory damages in lieu of actual damages and infringer’s profits, and the court entered judgment in the total amount of \$1,220,000. As discussed in greater detail in Section III.C.6(b)(1)(iii).v below, the defendants’ subsequent motions for JMOL, new trial and/or remittitur were denied, except Getty’s motion for JMOL with respect to Section 1202(b) liability was granted. AFP and Getty remained jointly liable for \$1.2 million in statutory damages, and AFP was held individually liable for \$10,000 of

¹⁶⁵⁴ Id. at 610-11.

¹⁶⁵⁵ Agence France Presse v. Morel, 769 F. Supp. 2d 295, 305-06 (S.D.N.Y. 2011).

¹⁶⁵⁶ Agence France Presse v. Morel, 934 F. Supp. 2d 547, 574-78 (S.D.N.Y. 2013).

statutory damages under the CMI provisions of the DMCA (one half of the total the jury awarded against AFP and Getty).¹⁶⁵⁷

j. Scholz Design v. Custom Homes

In this case the plaintiff brought a claim under Section 1202 for removal of CMI based on the defendant's posting on a web site of copies of images depicting designs of homes that the plaintiff claimed a copyright in. The plaintiff claimed that the defendant had removed the plaintiff's name from the designs before posting them. The court ruled that the designs were not copyrightable as architectural drawings because they did not contain the necessary level of detail to allow construction of a home from them. The court then dismissed the plaintiff's CMI claim, ruling that it must have a valid copyright infringement claim in order for its Section 1202 claim to survive.¹⁶⁵⁸

k. Personal Keepsakes v. PersonalizationMall.com In this case the plaintiff, operator of a web site selling personalized gifts and knickknacks, brought a claim against the defendants who also operated sites selling personalized gifts on the Internet for allegedly taking the plaintiff's copyrighted poems and incorporating them into the defendants' own products. Among other things, the plaintiff brought a claim under Section 1201 for removal of CMI from the poems when they were copied into the defendants' products. The plaintiff identified three pieces of purported CMI that one or more of the defendants removed when copying the poems: the poetrygift.com name affiliated with the poems on the plaintiff's site, the titles of the works (specifically, "Baptism Gifts"/"On Your Baptism Day" and "Ring Bearer Gift"/"To Our Ring Bearer"), and the copyright notice on every page of the plaintiff's web site.¹⁶⁵⁹

The court rejected all bases for the CMI claim. The court held that the poetrygift.com name could not be CMI because the copyright registrations attached to the complaint showed Personal Keepsakes, Inc., not poetrygift.com, as the owner of the copyright. Thus, poetrygift.com was at best an indicator of the seller of the product, not of the copyright owner. The titles could not be CMI because the copyright registrations did not list the titles of the works as they appeared on the plaintiff's web site, but rather referred to them as "Personal Keepsakes VI" and "Personal Keepsakes X." One could therefore not search the copyright titles as used on the web site to see if they were registered. The court concluded that allowing a plaintiff to make a DMCA claim based on alleged CMI that does not link up in any way to the copyright registration would be an invitation to unfair litigation against parties who had tried to tread carefully to avoid copyright infringement.¹⁶⁶⁰

¹⁶⁵⁷ Agence France Presse v. Morel, 2014 U.S. Dist. LEXIS 112436 at *6-7, *10-29 (S.D.N.Y. Aug. 13, 2014).

¹⁶⁵⁸ Scholz Design, Inc. v. Sard Custom Homes, LLC, 2011 U.S. Dist. LEXIS 76663 at *2-3, *9-10 & *14 (D. Conn. July 15, 2011).

¹⁶⁵⁹ Personal Keepsakes, Inc. v. PersonalizationMall.com, 2012 U.S. Dist. LEXIS 15280 at *1-2, *17-18 (N.D. Ill. Feb. 8, 2012).

¹⁶⁶⁰ Id. at *18-19.

In addition, the copyright notice that appeared on every page of the plaintiff's web site was not CMI with respect to the allegedly copied poems. The web site notice read "Web Site and Original Verses – © (1991-2012)." The court found that, although it was plausible that the copyright notice referred to the poems at issue, the complaint did not suggest the poems at issue were "original verses" as referenced in the notice.¹⁶⁶¹

Finally, the court ruled that the plaintiff had stated a case of false CMI against one of the defendants, Personalizationmall.com, when it put a copyright notice in the name of its "Walk with Jesus Baptism Keepsake" that incorporated the same or a very similar poem as the plaintiff's product, and that copyright notice followed a line in the poem that formed the title "Walk with Jesus." Consequently, the court held that it was plausible that the notice could refer to the poem, and not the product as a whole. The court also rejected the plaintiff's argument that statements in each of the defendants' web site Terms of Use referencing that the content or intellectual property on the web site was owned by the defendants constituted false CMI in connection with the poems, because the Terms of Use statements were not close to the poems.¹⁶⁶² The court cited another district court decision requiring that a defendant must remove the CMI from the body or the area around the work to violate the DMCA, and concluded that "as a matter of law, if a general copyright notice appears on an entirely different webpage than the work at issue, then that CMI is not 'conveyed' with the work and no claim will lie under the DMCA. [The plaintiff] cannot base a DMCA claim on Defendants' general copyright notices placed elsewhere on the site."¹⁶⁶³

In a later opinion, one of the defendants, Techny Advisors, moved to dismiss the plaintiff's claims for copyright infringement and for removal of and use of false CMI in connection with Techny's gift product titled "On Your Confirmation Day," which the plaintiff alleged copied a one sentence verse from one of its products reading, "May the strength of the Holy Spirit be with you, guiding you every day of your life." The court dismissed the copyright infringement claim on the ground that the verse was not copyrightable.¹⁶⁶⁴ With respect to its CMI claims, the plaintiff identified three purported CMI that Techny removed when it copied the verse: the www.poetrygift.com name affiliated with the poems on the plaintiff's site, the title of the work ("On Your Confirmation Day"), and the copyright notice on every page of the plaintiff's web site. The court ruled that none of these three elements constituted CMI for very similar reasons as in the earlier opinion – the www.poetrygift.com was merely the name of the seller of the product and conveyed nothing about the copyright status of the product; the title of the work was not CMI because it was not the same as the title of the registered work in which the plaintiff claimed a copyright; and the copyright notice on each page of the plaintiff's web site

¹⁶⁶¹ *Id.* at *19-20.

¹⁶⁶² *Id.* at *20-22.

¹⁶⁶³ *Id.* at *23. The court gave the plaintiff an opportunity to amend its DMCA claims if it could do so in good faith based on the guidance in the opinion. *Id.*

¹⁶⁶⁴ Personal Keepsakes, Inc. v. Personalizationmall.com, Inc., 975 F. Supp. 2d 920, 922 & 924-25 (N.D. Ill. 2013).

was not within the body of or around the copyrighted verses so as to clearly pertain to the plaintiff's poems, rather than the web site itself.¹⁶⁶⁵

The court also dismissed the plaintiff's claim of false CMI against Techny. The plaintiff based the false CMI claim on the allegation that Techny posted a notice attributing copyright ownership in the infringed works to www.giftsforyounow.com or some other web sites as the copyright claimant. The court noted, however, that such copyright notice was not close to the poems on Techny's web site, but rather was at the bottom of every page of the web site in the generic web site footer. It was therefore not "conveyed with" the poems that were allegedly copied and could therefore not constitute false CMI with respect to the poems.¹⁶⁶⁶ "Even if Techny were guilty of copying, it would not be liable for displaying false CMI for placing a generic copyright notice on the bottom of its webpage and not on each individual short phrase."¹⁶⁶⁷

I. Frost-Tsuji Architects v. Highway Inn

In Frost-Tsuji Architects v. Highway Inn, Inc.,¹⁶⁶⁸ the plaintiff Frost-Tsuji Architects (FTA) was hired by Highway Inn to design and oversee the development of a restaurant in Honolulu. Highway Inn terminated its relationship with FTA and hired another architect. Another contractor, Bargreen Ellingson, was the kitchen equipment designer and contractor for Highway Inn's restaurant. FTA prepared a design for the kitchen of the restaurant and transmitted a CAD file for the kitchen to Highway Inn. Bargreen Ellingson used this CAD file to create at least 12 versions of CAD drawings. FTA alleged that Bargreen Ellingson intentionally removed FTA's copyright management information from these drawings in violation of Section 1202(b)(1).¹⁶⁶⁹

The court granted summary judgment to the defendants on the claim for removal of CMI. FTA had presented no evidence that any of the defendants removed or directed anyone else to remove FTA's CMI. With respect to its claim against Highway Inn, FTA relied on emails, attached to which were a .jpeg file of a floor plan for the restaurant and a floor color study for the restaurant. The floor plan and floor color study were both stamped with CMI of the replacement architect, and the floor color study also referred to Highway Inn. The court ruled that Highway Inn's possession of floor plans that FTA claimed were virtually identical to its work did not mean that anyone from the defendants removed or had anyone remove FTA's CMI from FTA's plans. Virtually identical plans could have been created by redrawing FTA's plans and not including FTA's CMI, but that would not involve any removal or alteration of CMI from FTA's original work.¹⁶⁷⁰

¹⁶⁶⁵ Id. at 928-29.

¹⁶⁶⁶ Id. at 929.

¹⁶⁶⁷ Id.

¹⁶⁶⁸ 2014 U.S. Dist. LEXIS 157560 (D. Haw. Nov. 7, 2014), aff'd, 700 Fed. Appx. 674 (9th Cir. 2017) (summary order).

¹⁶⁶⁹ Id. at *1-10.

¹⁶⁷⁰ Id. at *12-14.

With respect to its claim against Bargreen Ellingson, FTA asserted that, after it was terminated, Bargreen Ellingson sent CADs out that did not include FTA's CAD containing its CMI. But the court ruled that sending out such CADs did not indicate that Bargreen Ellingson actually removed the CMI from FTA's work. FTA had not identified a drawing that it created from which FTA's CMI information was missing. Even if FTA were correct in contending that Bargreen Ellingson created its CAD for the kitchen design based on FTA's work, basing a CAD on FTA's CAD was not the same as "removing" CMI from a copyrighted work. The court noted that the physical act of removal is not the same as basing a drawing on someone else's work. The court therefore concluded that reliance on another's work is insufficient to support a claim of removal of CMI. Nor could the mere receipt and possession of a copyrighted work that has allegedly had CMI removed give rise to a violation of Section 1202(b)(1). Although such receipt and possession might be more consistent with a claim alleging the distribution of a copyrighted work with knowledge that CMI had been removed, such a claim had not been pled by the plaintiff.¹⁶⁷¹

Finally, the court noted that it had previously ruled that Highway Inn had an implied nonexclusive license to use FTA's copyrighted works. Other defendants used and adapted FTA's plans within the scope of that implied license. Therefore, even if one or more defendants removed FTA's CMI, no defendant could be said to have removed any CMI knowing or having reasonable grounds to know that the removal would induce, enable, facilitate, or conceal an infringement of copyright, as required by Section 1201(b)(1). Accordingly, the court granted summary judgment to the defendants with respect to the claim under Section 1201(b)(1).¹⁶⁷²

On appeal, the Ninth Circuit issued a summary order affirming the district court's grant of summary judgment on the CMI removal claim for the reasons stated in the district court's order entered Nov. 7, 2014.¹⁶⁷³

m. Tomelleri v. Zazzle, Inc.

The plaintiff was the owner of copyrights in highly realistic fish illustrations. The defendant operated a website entitled zazzle.com that allowed third party users to create, buy, and sell customized merchandise online. Users were able to upload an image to zazzle.com and create certain products to be made available on the web site, such as T-shirts or mugs, with that image on them. Zazzle.com then manufactured the user's customized product. The user could publish such products for sale through the user's "storefront" on the web site. The plaintiff claimed that sixty-two of his fish illustrations were copied without authorization and placed on zazzle.com. The copied illustrations appeared in five books that the plaintiff had registered with the Copyright Office. Each of the five books listed the plaintiff as the author or illustrator of the book on the cover. Each book also contained a statutory copyright notice within the first few pages of the book. Four of the five books, however, did not identify the plaintiff as the author or

¹⁶⁷¹ Id. at *15-20.

¹⁶⁷² Id. at *20-22.

¹⁶⁷³ Frost-Tsuji Architects v. Highway Inn, Inc., 700 Fed. Appx. 674 (9th Cir. 2017) (summary order).

copyright holder immediately adjacent to each fish illustration within the book. The fifth book contained a copyright symbol and the plaintiff's name under each illustration.¹⁶⁷⁴

The plaintiff brought claims against the defendant for direct and indirect copyright infringement and for false CMI and removal of CMI under Section 1202. After the plaintiff filed a first amended complaint, the defendant filed a motion to dismiss. The court subsequently entered a pretrial order and the defendant then filed a motion for summary judgment. Because of this odd procedural posture of the case, the court elected to first address the defendant's legal bases for its summary judgment motion. Then, to the extent there were any remaining claims after the summary judgment motion rulings, the court addressed them in the context of the motion to dismiss.¹⁶⁷⁵

Turning to the motion for summary judgment on the plaintiff's Section 1202 claims, the court granted the defendant's motion for summary judgment on the Section 1202(a) claim. The plaintiff contended the defendant was liable under Section 1202(a) because the simple act of placing an image on zazzle.com without the surrounding CMI of the plaintiff's books or the plaintiff's web site on which some of the illustrations also appeared, removed author-identifying CMI. The court rejected this argument, noting other decisions had held that the mere appearance of an image on a web site does not convey CMI for that image – web sites generally do not claim ownership or authorship over an image just because the image appears on the web site. Thus, the mere fact that the defendant's illustrations appeared on the plaintiff's web site did not convey false CMI.¹⁶⁷⁶

The only other information the plaintiff alleged was false CMI was the phrase "Image licensed to Zazzle Inc. All unauthorized use is prohibited," which the defendant placed in the metadata of each image uploaded onto the site. The court declined to decide whether that phrase met the statutory definition of CMI, instead noting that the plaintiff had not come forward with any evidence showing that the defendant added that phrase with the intent to induce infringement, as required by Section 1201(a). The court noted that the defendant had invested significant resources to remove any designs on its web site accused of infringement, and the plaintiff had

¹⁶⁷⁴ *Tomelleri v. Zazzle, Inc.*, 2015 U.S. Dist. LEXIS 165007 at *2, *7-8 & *11-12 (D. Kan. Dec., 9, 2015).

¹⁶⁷⁵ *Id.* at *1 n.1, 14. The defendant grouped the plaintiff's claims for direct infringement into three groups. The first group consisted of 127 product designs with fish images that were simply silhouettes of fish. The court granted the defendant summary judgment on this group because the plaintiff measured each fish specimen and drew the outline of each fish so that the specimen's exact proportions were present in the illustration. The outlines were therefore uncopyrightable facts. The second group consisted of eight product designs with line art images depicting a fish. The court granted summary judgment as to this group because, again, the outline of the fish in the plaintiff's illustrations was not copyrightable, and once the outline was removed from the plaintiff's illustration, there was nothing left to compare to the product designs under the substantial similarity test. The third group consisted of images that were much more detailed than the first two groups. The court denied summary judgment as to this group because there were fact issues as to whether the plaintiff's choice of colors and details beyond those normally found on the species depicted were sufficiently creative to support a copyright. *Id.* at *30-35.

¹⁶⁷⁶ *Id.* at *36-37.

not pointed to a single fact that created a genuine issue of material fact showing otherwise. According, the defendant was entitled to summary judgment on the plaintiff's Section 1201(a) claim.¹⁶⁷⁷

The court then turned to the plaintiff's claims for removal of CMI under Section 1202(b). The defendant contended it was entitled to summary judgment on this claim on the ground that the statutory copyright notices at the beginning of the books at issue in the litigation were not CMI because the notices were not conveyed in connection with the plaintiff's illustrations. Because neither the Tenth Circuit nor any district court within the Tenth Circuit had previously addressed the definition of CMI, the defendant asked the court to adopt the Eastern District of Pennsylvania's ruling the Schiffer case, discussed in Section II.G.1(b)(2)(ii).a below, which ruled that copyright notices on the inside of book covers did not constitute CMI for the individual photographs inside the books, and that to constitute CMI the information must be in the body of, or the area around, the copyrighted work itself. The court declined to follow the Schiffer ruling, deciding that the phrase "conveyed in connection with copies ... of the work" in the definition of CMI does not require that the information be located immediately adjacent to the image. The court also noted that, in addition to the statutory copyright notice, both the cover and title page of the books at issue stated that the illustrations were by the plaintiff, and the court found it implausible that an individual reading those books would not understand such a statement to apply to all of the illustrations within the book. Because the plaintiff stated in an affidavit that many of his images uploaded to zazzle.com were scanned from the books at issue in the case, there was a genuine issue of material fact regarding whether the plaintiff had met the statutory definition of CMI with respect to the copyright notices and the front cover statements that credited the illustrations to the plaintiff.¹⁶⁷⁸

The defendant also contended that there was no identifying information that qualified as CMI with regard to the metadata included in the electronic image files uploaded to zazzle.com. The court noted that the plaintiff had not come forward with any evidence that showed the images on his web site that were allegedly copied and uploaded to zazzle.com contained metadata with identifying information that satisfied the definition of CMI. Therefore, to the extent the plaintiff claimed that the defendant violated Section 1202(b) through the alteration and removal of CMI in metadata included in the electronic image files of his illustrations, the court granted summary judgment in the defendant's favor. The court further granted summary judgment that the defendant could not be liable under Section 1202(b)(1) specifically, because the plaintiff had not come forward with any evidence showing that the defendant itself uploaded his fish illustrations to zazzle.com, much less evidence showing that the defendant intentionally removed CMI.¹⁶⁷⁹

The court then turned to the defendant's motion to dismiss, finding that, in view of the court's summary judgment rulings, the only issue left to decide was whether the plaintiff's claim

¹⁶⁷⁷ Id. at *37-38.

¹⁶⁷⁸ Id. at *39-41.

¹⁶⁷⁹ Id. at *41-43.

under Section 1202(b) was limited to CMI located within metadata or if it included additional CMI associated with the plaintiff's illustrations. Although the plaintiff's amended complaint discussed CMI only in the context of metadata, the plaintiff contended in the pretrial order that his fish illustrations had been published in books, that all of those books contained a copyright notice and title pages, and that the defendant violated Section 1202 in part by removing information initially displayed in connection with the plaintiff's works. Construing these allegations liberally, the court ruled that they were sufficient to extend the plaintiff's Section 1202(b) claim to CMI that was contained in information other than metadata. Therefore, the court allowed the plaintiff's claim to proceed under Section 1202(b) in regard to CMI altered or removed from the books in which the plaintiff's illustrations appeared.¹⁶⁸⁰

In addition to the Section 1202 claims, the court also ruled on the defendant's motion for summary judgment with respect to the plaintiff's claims for contributory infringement. The court noted that material contribution is established for a contributory infringement claim by showing that the defendant had knowledge of the infringing activity of another and encouraged or assisted the other's infringement, or provided machinery or goods that facilitated the infringement. The defendant argued it was entitled to summary judgment because the plaintiff had not shown that the defendant had actual knowledge of specific infringing material available on zazzle.com and failed to remove it from the web site. The court rejected this argument, noting that the plaintiff had stated in his affidavit that after he gave the defendant notice of the allegedly infringing material on zazzle.com, some of that material remained on the web site for six to nine months. In response, the defendant claimed that it promptly removed every product design it believed might contain the plaintiff's illustrations and that it did not have actual notice of specific infringing material because the plaintiff did not use the "report this product" button on the plaintiff's web site to report the potentially infringing product designs. The court concluded that there was therefore a genuine issue of fact and denied the defendant's motion on the plaintiff's contributory infringement claim.¹⁶⁸¹ The court noted in a footnote, citing Justice Ginsburg's concurrence in the Grokster case, that the Supreme Court had articulated a "second test to prove contributory infringement" based on Sony, under which liability can be imposed for distributing a product distributees use to infringe copyrights, if the product is not capable of substantial or commercially significant noninfringing uses. The district court noted it need not address this test because the plaintiff did not appear to assert that the defendant was liable under it.¹⁶⁸²

Finally, the court granted summary judgment to the defendant on the vicarious liability claim because the plaintiff had not come forward with sufficient evidence for a reasonable juror to conclude that the infringing activity was a draw for users on zazzle.com.¹⁶⁸³

¹⁶⁸⁰ Id. at *58-59.

¹⁶⁸¹ Id. at *44-46.

¹⁶⁸² Id. at *45 n.62.

¹⁶⁸³ Id. at *47-48.

n. Iconics v. Massaro

In this case, the defendant Massaro left the employment of the plaintiff Iconics and took Iconics source code without permission. Iconics alleged that Massaro copied some of that source code into a new product he helped develop for a third party named Volpe Industries. Iconics brought claims under the DMCA, alleging that Massaro first removed CMI from the copied source code modules in the form of headers, in violation of Section 1202(b), and then replaced them with false CMI, in violation of Section 1202(a). Iconics moved for summary judgment on its DMCA claims.¹⁶⁸⁴

The CMI that Iconics alleged had been removed was headers in its source code files comprising proprietary notices such as “Copyright (c) 1986-2006 ICONICS, Inc. (copyrighted as an unpublished work). CONFIDENTIAL: Contains TRADE SECRET information,” together with the name of the original author of the file. Iconics alleged that Massaro transferred Iconics source code files onto servers of Volpe Industries, removed the copyright headers and replaced them with new Volpe headers. Iconics also asserted that the code itself in the files often referred to Iconics as “Ico” and that those references were replaced in the code itself with “Fox” (for Volpe Industries’ “Project Foxtrot”). The court ruled that the copyright headers were paradigmatic CMI and that in the software code context, even information integrated into the code itself can also be CMI, where it reveals authorship.¹⁶⁸⁵ The in-line references to “ico” and “fox” were therefore also CMI. The court rejected the defendants’ argument that headers on individual files could not be CMI when the copyright at issue covered the full versions of programs, not individual files. The court noted that the definition of CMI neither states nor implies that CMI can exist only with regard to the full version of a work, instead requiring only that the information be conveyed in connection with copies of a work.¹⁶⁸⁶

It was uncontested that for at least two files, Massaro deleted an Iconics copyright header and replaced it with a Volpe Industries copyright header. Whether Massaro did so for 280 other Iconics source code files was contested. However, the defendants raised two arguments in opposition to summary judgment. First, they argued that Massaro did not “provide” or “distribute” false CMI because he uploaded the false CMI only onto the private Volpe server, rather than broadcasting it more widely. The court rejected this argument, noting that courts have not held that “distribution” under Section 1202(a) requires wide, public distribution. And even if Massaro had not “distributed” the false CMI, he surely had “provided” it.¹⁶⁸⁷

Second, the defendants argued that there was insufficient evidence of intent and knowledge, as Massaro had testified that he believed he was permitted to use the code in

¹⁶⁸⁴ Iconics, Inc. v. Massaro, 192 F. Supp. 3d 254, 259-60, 271-72 (D. Mass. 2016).

¹⁶⁸⁵ Id. at 272 (citing Bounce Exchange, Inc. v. Zeus Enterprise Ltd., 2015 U.S. Dist. LEXIS 165073 at *3 (S.D.N.Y. Dec. 9, 2015), discussed in Section II.G(b)(1)(ii).k above).

¹⁶⁸⁶ Iconics, 192 F. Supp. 3d at 272.

¹⁶⁸⁷ Id. at 272-73.

question for non-competitive side projects, which he believed Project Foxtrot to be. He also testified that he replaced the Iconics headers with Volpe headers only after learning that Iconics was upset with him, as an attempt to separate the two companies' code. Iconics argued that such testimony was not credible enough to raise a genuine issue of material fact, because Massaro changed only the headers, not the substance of the code, and made the changes secretly after being confronted by Iconics. The court ruled that, while these facts raised serious questions about Massaro's testimony, they were fundamentally credibility determinations inappropriate for summary judgment. Because a genuine dispute existed over Massaro's intent, the court denied summary judgment on Iconics' DMCA claims.¹⁶⁸⁸

o. Stevens v. CoreLogic

CoreLogic developed and provided software to Multiple Listing Services (MLSs). Real estate agents used CoreLogic's software platform to upload their real estate listings to an MLS, including property descriptions and photographs. The plaintiffs were professional photographers who took photos of houses for sale and licensed the photos to real estate agents to upload to an MLS. In describing the background of the case, the court noted that some photographers embed CMI in metadata attached to their photos. Some digital cameras can be used to automatically create Exchangeable Image File Format (EXIF) metadata. Not all cameras are configured to include metadata, and not all photographs produced by the plaintiffs had CMI in their metadata. Images uploaded to CoreLogic's MLS platforms could be manipulated before or after uploading. Manipulations could include resizing, rotating, cropping and adjusting resolution of the image, all of which could result in inadvertent removal of the embedded metadata. Embedded metadata could also be removed inadvertently by email programs, opening an image on an iPhone using iOS Safari, or pasting the image in some versions of Microsoft Word. Before late 2014 or early 2015, CoreLogic's platforms removed all EXIF metadata from the photos uploaded to the MLS. In late 2014 or early 2015, CoreLogic rewrote the code so that EXIF metadata was preserved during download. The plaintiffs brought claims under the anti-circumvention provisions with respect to several of their photos that were uploaded using the CoreLogic platform and CoreLogic moved for summary judgment.¹⁶⁸⁹

The plaintiffs alleged that CoreLogic distributed false CMI because CoreLogic displayed its own copyright notice on the same web page as the plaintiffs' photos. The court granted CoreLogic summary judgment on this claim under Section 1202(a), citing several decisions finding that a copyright notice on the same page as a plaintiff's photos is insufficient to show false information based solely on proximity of the notice to the plaintiff's photo.¹⁶⁹⁰

With respect to a claim for removal of CMI under Section 1202(b)(1), the court noted that the plaintiffs must prove that CMI was on the photos uploaded to the MLS, CoreLogic took

¹⁶⁸⁸ *Id.* at 273.

¹⁶⁸⁹ *Stevens v. CoreLogic, Inc.*, 194 F. Supp. 3d 1046 at 1047-48 (S.D. Cal. 2016), *aff'd*, 899 F.3d 666 (9th Cir. Aug. 6, 2018).

¹⁶⁹⁰ *Id.* at 1051-52.

action that removed or altered the CMI, and any action by CoreLogic was intentional. The court concluded the plaintiffs had failed to make the necessary proof on all three points. First, there was no evidence that the photos at issue had CMI at the time they were uploaded. Although the plaintiffs testified that some of their photos had CMI in the metadata at the time the photos were given to a real estate agent, there was insufficient evidence as to what happened to the photos *after* delivery to the agent, and there were several different ways CMI could have been excised before upload. Although it was clear that CoreLogic's platform would have removed CMI metadata had it existed at the time of upload, the plaintiffs could not point to a single photo that had CMI at the time of upload. Second, the plaintiffs had not shown that CoreLogic removed or altered any CMI. CoreLogic was just the software developer and did not select or control the photos to be uploaded. Nor did it control whether or not the photos had CMI. The act of uploading, which was what the plaintiffs alleged led to the removal of CMI, was done by a third party actor. Third, the plaintiffs had presented no evidence that CoreLogic intentionally removed CMI, as opposed to removal being an unintended side effect of the fact that the software platform was based on a software library that failed to retain metadata by default. Accordingly, CoreLogic was entitled to summary judgment on the plaintiffs' Section 1202(b)(1) claim.¹⁶⁹¹

The court ruled that the plaintiffs' claims under Sections 1202(b)(2) and (3) for distribution of images missing CMI must fail because the plaintiffs presented no evidence (1) that CoreLogic knew or had reason to know that distributing images without CMI would induce, enable, facilitate or conceal an infringement and (2) that any distribution was done without the authority of the copyright owner. With respect to the first requirement, the court noted the CMI in the metadata was not generally visible in the image itself but could be accessed and viewed using computer programs that were capable of displaying EXIF metadata. There was no evidence that, had the CMI metadata been embedded in the photos, this might have prevented infringement, and that CoreLogic knew it would help prevent infringement. Nor had the plaintiffs provided evidence that the absence of metadata led to actual copyright infringement or that they had ever used metadata to track down copyright infringers.¹⁶⁹²

With respect to the second requirement, the court noted the plaintiffs licensed their photos to real estate agents for the express purpose of uploading them onto an MLS, and knew the agents would be manipulating the photos specifically so they could be used on the MLS. Agents paid the plaintiffs for this use. The plaintiffs knew that the MLS had software used by the agents to upload the photos and agreed the agents could use the photos in this manner. Nowhere in the agreements with the agents did the plaintiffs warn the agents not to remove embedded metadata not viewable with the naked eye. To the extent there was CMI on the photos, to the extent CoreLogic excised that CMI or knew the CMI had been excised, to the extent CoreLogic's removal or distribution of the CMI was intentional – all of which the plaintiffs had failed to prove – the plaintiffs impliedly gave authority to the agents to upload the photos

¹⁶⁹¹ *Id.* at 1052-53.

¹⁶⁹² *Id.* at 1053.

even though the result was the removal of CMI. Accordingly, the court granted summary judgment to CoreLogic on the plaintiffs' Section 1202(b)(2) and (3) claims.¹⁶⁹³

On appeal, the Ninth Circuit affirmed. The court held that Sections 1202(b)(1) and (b)(3) both require an affirmative showing that the defendant possesses the mental state of knowing, or having a reasonable basis to know, that its actions will induce, enable, facilitate, or conceal infringement. The court found that the plaintiffs had not offered any evidence to satisfy that mental state requirement. Their primary argument was that, because one method of identifying an infringing photograph had been impaired (removal of the metadata files), someone *might* be able to use their photographs undetected. That assertion rested on no affirmative evidence at all, but rather simply identified a general possibility that existed whenever CMI is removed. Such a generic approach is insufficient under Section 1202(b) – there must be specific allegations as to how identifiable infringements “will” be affected.¹⁶⁹⁴

The court elaborated, however, that as the statute is written in the future tense, the plaintiffs need not show that any specific infringement had already occurred. Statutes requiring knowledge that a future action “will” occur do not require knowledge in the sense of certainty as to a future act. Rather, the court held, a plaintiff bringing a Section 1202(b) claim must make an affirmative showing, such as by demonstrating a past pattern of conduct or *modus operandi*, that the defendant was aware or had reasonable grounds to be aware of the probable future impact of its actions. The plaintiffs' bare assertion that, when CMI metadata is removed, copyright infringement plaintiffs lose an important method of identifying a photo as infringing, was insufficient to satisfy the knowledge requirement. Instead, the plaintiffs were required to provide evidence from which one could infer that future infringement is likely, albeit not certain, to occur as a result of the removal or alteration of CMI.¹⁶⁹⁵

Here, the plaintiff had failed to offer any specific evidence that removal of CMI metadata from their photographs would impair their policing of infringement. They had not, for example, averred that they had ever used CMI metadata to prevent or detect copyright infringement (and in fact there was testimony to the opposite), much less how they would do so. Nor had they brought forth any evidence indicating that CoreLogic's *distribution* of real estate photographs ever induced, enabled, facilitated, or concealed any particular act of infringement by anyone, let alone a pattern of such infringement likely to recur in the future. And the court observed that a party intent on using a copyrighted photograph undetected could itself remove any CMI metadata, precluding detection through a search for the metadata. Thus, on the current record, one could not plausibly say that removal by a third party of metadata “will” make it easier to use

¹⁶⁹³ *Id.* at 1053-54.

¹⁶⁹⁴ *Stevens v. CoreLogic, Inc.*, 899 F.3d 666, 672-73 (9th Cir. 2018) (amended opinion).

¹⁶⁹⁵ *Id.* at 673-75.

a copyrighted photograph undetected, using “will” in the predictive sense the court had elaborated. Accordingly, summary judgment for CoreLogic was correctly granted.¹⁶⁹⁶

p. Friedman v. Live Nation Merchandise

In Friedman v. Live Nation Merchandise,¹⁶⁹⁷ the defendant Live Nation stipulated to copyright infringement liability for unauthorized use of the plaintiff’s copyrighted photos of the hip hop group Run-DMC on t-shirts and calendars. Live Nation then moved for partial summary judgment on the plaintiff’s additional claim for liability under Section 1202(b) for the distribution of works knowing that CMI had been removed or altered without authority of the copyright owner or the law. The district court granted Live Nation’s motion and the plaintiff appealed that grant, as well as the district court’s ruling with respect to the amount of statutory damages that the plaintiff could recover for the copyright infringement.¹⁶⁹⁸

The Ninth Circuit reversed the grant of summary judgment against the plaintiff’s CMI claim. The district court had granted summary judgment to Live Nation on the ground that the plaintiff had made no factual showing that Live Nation either removed the CMI in question or did so knowingly. The Ninth Circuit noted that the district court had focused on the wrong question. Although the statute does prohibit the intentional removal of CMI, the plaintiff could also prevail upon a showing that Live Nation distributed his works with the knowledge that CMI had been removed, even if Live Nation did not remove it. And the court found that there was sufficient circumstantial evidence in the record to create a triable issue of fact as to whether Live Nation distributed the plaintiff’s Run-DMC photos with the requisite knowledge.¹⁶⁹⁹

Specifically, the evidence showed that several of the plaintiff’s photos of Run-DMC had appeared in a book collecting his work. In 2005, he granted a license to Sony Music to reproduce some of his Run-DMC photos, accompanied by information indicating that he owned the copyrights, on a web site. The license permitted Sony to alter the images in some respects, and was the only license the plaintiff had granted that authorized alterations to his photos. The plaintiff produced the images as they appeared on Live Nation’s merchandise and the same images as they had appeared on Sony’s web site and in his book. In his motion for summary judgment, he compared them, demonstrating that there were striking similarities. For example, some of the photos used in Live Nation’s calendar included alterations that the plaintiff had authorized only for the Sony web site. And some of the photos appeared to have been scanned from his book, as they contained captions and other layout features that appeared in that source

¹⁶⁹⁶ Id. at 675-76.

¹⁶⁹⁷ 833 F.3d 1180 (9th Cir. 2016).

¹⁶⁹⁸ Id. at 1184.

¹⁶⁹⁹ Id. at 1187.

alone. The images on Live Nation’s products did not include copyright information that had been present on the earlier versions.¹⁷⁰⁰

The Ninth Circuit found there was sufficient circumstantial evidence as a whole to permit a reasonable inference that Live Nation knew of the removal of the CMI, especially given the fact that Live Nation had never offered any explanation of how it came to possess the images. A jury could therefore draw an inference that Live Nation knew of the removal of CMI when it distributed the plaintiff’s photos. The plaintiff had thus discharged his burden of production at summary judgment, and the burden shifted back to Live Nation to carry its ultimate burden of persuasion that there was no genuine issue of material fact. Live Nation might have done so by providing some explanation for how it came to possess the plaintiff’s images – missing their CMI – in the first place, establishing its lack of knowledge and negating the inference drawn from the juxtaposition of the photos. But it had not done so. The court also observed that how Live Nation came to possess the plaintiff’s photos – and thus whether it had knowledge that the CMI had been removed – was a fact particularly within Live Nation’s knowledge. It would therefore be unfair to burden the plaintiff at the summary judgment stage with proving that knowledge with greater specificity than he did. The court therefore reversed the district court’s grant of summary judgment to Live Nation on the CMI claim.¹⁷⁰¹

The court then turned to the district court’s denial of the plaintiff’s request for an award of statutory damages for each retailer that had distributed merchandise with the unauthorized photos on them. The district court ruled that the plaintiff was entitled to only one statutory damages award per infringed work. The Ninth Circuit affirmed this ruling. The court applied its ruling in Columbia Pictures,¹⁷⁰² which held (i) that when statutory damages are assessed against one defendant or a group of defendants held to be jointly and severally liable, each work infringed may form the basis of only one award, regardless of the number of separate infringements of that work, but (ii) where separate infringements for which two or more defendants are not jointly liable are joined in the same action, separate awards of statutory damages would be appropriate. The plaintiff argued that the retailers to whom Live Nation distributed infringing merchandise were each jointly and severally liable for infringement with Live Nation, but not with each other, thus entitling him to a separate award for each “unit” of infringers jointly and severally liable.¹⁷⁰³

The Ninth Circuit rejected this argument, noting that the holding in Columbia Pictures was premised on the fact that each of the downstream infringers for whom the plaintiff received a separate damages award was a defendant in the case, and those parties had been adjudicated liable for infringement, and jointly and severally liable with another infringer. Such was not true

¹⁷⁰⁰ Id. at 1182-83, 1188.

¹⁷⁰¹ Id. at 1188-89.

¹⁷⁰² Columbia Pictures Television v. Krypton Broadcasting of Birmingham, Inc., 106 F.3d 284 (9th Cir. 1997), rev’d on other grounds sub nom. Feltner v. Columbia Pictures Television, Inc., 523 U.S. 340 (1998).

¹⁷⁰³ Id. at 1184, 1190-91.

in this case. Section 504(c)(1) provides for an award of statutory damages for all infringements “involved in the action,” and any downstream infringements could not be “involved in the action” unless the alleged infringers responsible for those infringements were joined as defendants in the case, and the particular alleged infringements involving them adjudicated. A plaintiff seeking separate damages awards on the basis of downstream infringement must therefore join the alleged downstream infringers in the action and prove their liability for infringement. Because the plaintiff did not join any of his alleged downstream infringers as defendants, the district court correctly held that he was limited to one award per work infringed by Live Nation.¹⁷⁰⁴

q. Robert L. Stark Enterprises v. Neptune Design Group

In Robert L. Stark Enterprises, Inc. v. Neptune Design Group, LLC,¹⁷⁰⁵ the defendant, an architectural firm, created design plans for the plaintiff to use to build a number of franchised stores. The plaintiff became dissatisfied with the defendant’s work and hired a new architectural firm. The plaintiff provided the new firm with a copy of the defendant’s store plans in PDF format and the new firm had the PDF file converted into a CAD file. The defendant brought claims against the plaintiff under Section 1202, arguing that the conversion of the copies of the defendant’s design plans from PDF to CAD format impermissibly removed CMI. The plaintiff brought a declaratory judgment action against the defendant seeking a declaration that it did not improperly remove CMI and sought summary judgment on the issue.¹⁷⁰⁶

The new architectural firm, through a third party CAD firm, created the CAD file using layering instructions provided by the new architectural firm. The plaintiff argued that the relevant testimony showed the CAD process did not “remove” CMI. Rather, information was inputted into the architectural firm’s layering system, which produced a new work that was not an exact copy of the defendant’s original work. Therefore, at no point did anyone “remove” CMI. The plaintiff further argued that the defendant could not establish actual knowledge of unauthorized removal. The defendant argued that the definition of removal should not be so narrowly construed. Rather, the court should not require that a party physically remove the CMI. The defendant argued the evidence established that the plaintiff performed acts of removal through its agent, the new architectural firm, to whom the plaintiff sent the PDF file. The new firm converted the PDF file to CAD form, then used the CAD file to create sixteen additional franchised stores whose plans were strikingly similar to the defendant’s works, yet the CAD file did not display the defendant’s CMI. The court noted that, in essence, the defendant was arguing that the new firm removed the CMI and then created derivative works without retaining the defendant’s CMI on those derivative works.¹⁷⁰⁷

¹⁷⁰⁴ Id. at 1191-92.

¹⁷⁰⁵ 2017 U.S. Dist. LEXIS 55951 (N.D. Ohio Apr. 12, 2017).

¹⁷⁰⁶ Id. at *1-2, *5-7, & *14.

¹⁷⁰⁷ Id. at *30-31.

The court found the plaintiff was entitled to summary judgment. The plaintiff had admittedly sent the defendant's copyrighted plans to the new architectural firm, which then scanned the documents into its system. To the extent those actions could arguably constitute copying, there was no evidence suggesting that the CMI was removed during that process. Accordingly, those actions were not sufficient to establish a violation of the DMCA. The court further found that the defendant had failed to point to a genuine issue of material fact with regard to the removal of the CMI during the CAD conversion process. An employee of the new architectural firm testified that the firm modified the materials in order to conform them to the firm's layering system. Thus, the program did not "copy" the materials, but rather created a digital layer similar to overlay drafting, and the layering instructions resulted in changes to the materials based on the layering system employed. Although the defendant generically argued that the plans created from this process were strikingly similar, the defendant had wholly failed to show that the resulting works were "copies" of the defendant's copyrighted work. Because there was no evidence that the plaintiff or its agents removed CMI from the defendant's original work or "distributed" a "copy" of the defendant's work knowing that CMI had been removed, summary judgment in favor of the plaintiff was warranted.¹⁷⁰⁸

r. Gattoni v. Tibi, LLC

In Gattoni v. Tibi, LLC,¹⁷⁰⁹ the plaintiff owned a photograph that the defendant copied, cropped and posted to its Instagram page. The post was accompanied by the caption "Palette," an image of a camera, a colon, and a hyperlinked reference to the plaintiff's Instagram page. The plaintiff brought a claim under Section 1202(b) based on the fact that the defendant's cropping had removed the plaintiff's copyright notice from the photo. The defendant brought a motion to dismiss under Fed. R. Civ. Pro. 12(b)(6), which the court denied.¹⁷¹⁰ Although the plaintiff alleged only that CMI existed on her photograph that identified her as the owner of the photograph, the court noted that the complaint was bolstered by exhibits showing that the defendant's post omitted the copyright notice "(c) Matilde Gattoni Photograph, 2016, All rights reserved," which the plaintiff had included with her post. With respect to Section 1202(b)'s requirement of intent, the court noted that the presence of a credit "tag" on the defendant's post that hyperlinked to the plaintiff's Instagram page undermined the strength of the plaintiff's allegations regarding the defendant's intent. However, the defendant had cited no authorities that "tagging" the author of a photograph conclusively meant the defendant lacked the required scienter under Section 1201(b). Because the court was required to draw all reasonable inferences in the plaintiff's favor at the motion to dismiss stage, the court denied the motion.¹⁷¹¹

s. The Art of Design v. Pontoon Boat

¹⁷⁰⁸ Id. at *31-32.

¹⁷⁰⁹ 254 F. Supp. 3d 659 (S.D.N.Y. 2017).

¹⁷¹⁰ Id. at 660-61.

¹⁷¹¹ Id. at 664-65.

In this case the plaintiff owned custom artwork that could be applied to boats, motorcoaches, airplanes, helicopters and recreational vehicles. The defendant engaged the plaintiff to apply its designs to the exterior of a limited number of pontoon boats. The plaintiff alleged that sometime after the transaction was completed, the defendant continued to market, sell and distribute products displaying the designs, or substantially similar designs, without authorization and without the notice that the plaintiff had applied to its original designs, which read: “TAOD DESIGNS ARE THE PROPERTY OF TAOD. THEY ARE NOT TO BE REPRODUCED, COPIED OR FORWARDED TO ANYONE WITHOUT WRITTEN PERMISSION.” The plaintiff claimed that the notice constituted CMI and that by removing it from the unauthorized copies, the defendant was in violation of Section 1202. The defendant moved to dismiss.¹⁷¹²

The court granted the motion. The court noted that, while the alleged CMI notice claimed that “TAOD” owned the labeled designs, the registrations of the designs with the Copyright Office were in the names of “The Art of Design, Inc.” and “Dean Loucks” as the owners. Thus, if one were to see the designs with the CMI notice on them in the name of “TAOD,” and search for that owner to verify the graphics’ copyright status, the search would come up empty, because the actual owners are The Art of Design, Inc. and/or Dean Loucks. The court noted that the problem was magnified in this instance by the additional fact that there were no entities named simply “TAOD” registered in the State of Indiana. Therefore, the notice the plaintiff placed on its designs did not accomplish the purpose of CMI, which is to inform the public that something is copyrighted and to prevent infringement, and thus did not qualify as CMI. Accordingly, the court dismissed the plaintiff’s claim with prejudice.¹⁷¹³

t. Fischer v. Forrest

In this case, the plaintiff, an apiarist, sold a product to aid in honey harvesting known as Bee-Quick. He used the following phrases in conjunction with the sale of Bee-Quick on his website:

- Are you tired of your spouse making you sleep in the garage after using Butyric Anhydride?
- Are you tired of using hazardous products on the bees you love?
- Fischer’s Bee-Quick is a safe, gentle, and pleasant way to harvest your honey.
- A Natural, Non-Toxic Blend of Oils and Herbal Extracts

For a time, the defendants sold Bee-Quick through their web site, but then switched over to selling an alternative product known as Natural Honey Harvester. The plaintiff asserted claims under Section 1202, alleging that the defendants had removed CMI from his copyrighted works

¹⁷¹² The Art of Design, Inc. v. Pontoon Boat, LLC, 2017 U.S. Dist. LEXIS 133672 at *2-4, *14 (N.D. Ind. Aug. 22, 2017).

¹⁷¹³ Id. at *14-15.

in the course of marketing of the Natural Honey Harvester. The defendants moved for summary judgment.¹⁷¹⁴

The court began its analysis by noting that CMI must be attached to, depicted in, or broadly conveyed in connection with a copyrighted or copyrightable work. The court noted that Fischer had oscillated in his theories under the DMCA, but drawing on his various filings, four items could potentially serve as an original “work” of Fischer’s from which the defendants allegedly removed CMI: 1) the web site and/or brochure Fischer submitted in conjunction with his copyright registration; (2) the description text of the Bee-Quick product that Fischer sent to the defendants; (3) the four copyrighted phrases listed above, variants of which the defendants had used in an allegedly offending advertisement; and (4) the phrase to which “Fischer’s” was attached in an advertisement altered by the defendants: “Fischer’s Bee-Quick is a safe, gentle, and pleasant way to harvest your honey.” The court considered each in turn.¹⁷¹⁵

With respect to (1), Fischer testified that the defendants removed four sentences from his brochure and that various “epigrams” relating to his product could be found on various web pages of the defendants. The court ruled that Fischer could not maintain a claim for removal of CMI on these bases because no CMI was removed from his original brochure, his web site, or a copy or display of them. Fischer’s brochure and web site were not copied by the defendants, and the defendants’ advertisement bore no resemblance to Fischer’s brochure or web site. Aside from the four discrete phrases noted above among the many used on Fischer’s brochure and web site, there was no similarity between Fischer’s original works and the defendants’ advertisement for the Natural Honey Harvester. The defendants could therefore not be said to have removed CMI from those of Fischer’s “works” in the course of copying them.¹⁷¹⁶

With respect to (2), Fischer had not shown that the defendants removed CMI from the description text, because, at the summary judgment stage, Fischer did not adduce evidence of the content of the description text he had sent to the defendants. Moreover, Fischer’s affidavits and the complaint suggested that the defendants’ work at issue here was an advertisement based upon an earlier advertisement which in turn drew upon various materials Fischer sent to the defendants. But Fischer had not cited any case support that DMCA liability encompasses that sort of composite “work.” Rather, Fischer’s claim instead would sound, if at all, in copyright infringement.¹⁷¹⁷

With respect to (3), the four phrases that the defendants modified and used were not of a character designed to inform the public that a work is copyrighted and by whom, which is the purpose of CMI. Only one of the phrases even referred to Fischer. The court found that no reader would perceive that the word “Fischer’s” as used in the phrase “Fischer’s Bee-Quick is a

¹⁷¹⁴ Fischer v. Forrest, 286 F. Supp. 3d 590, 596-97, 599 (S.D.N.Y. 2018), aff’d, 968 F.3d 216 (11th Cir. 2020), cert. denied, 142 S. Ct. 460 (2021).

¹⁷¹⁵ Id. at 608-09.

¹⁷¹⁶ Id. at 609.

¹⁷¹⁷ Id. at 609-10.

safe, gentle, and pleasant way to harvest your honey” spoke to copyright ownership. No reader would find that such a product descriptor signaled that a “James H. Fischer” or even someone named “Fischer” was the copyright holder of the phrase to which it was attached and those surrounding it. The sentence instead advertised Fischer’s product, and fairly conveyed that Fischer was the owner and/or producer of that product. But neither that phrase, nor the other three at issue, conveyed Fischer’s authorship or copyright ownership of those expressions. The phrases therefore did not constitute CMI.¹⁷¹⁸

With respect to (4), for the same reasons, the defendants’ replacement of the word “Fischer’s” with “Natural Honey Harvester” in their advertisement’s phrase “Natural Honey Harvester is a safe, gentle, and pleasant way to harvest your honey” was not an act of CMI removal, because the word “Fischer’s” had no CMI significance as used in the advertisement. The court therefore granted the defendants summary judgment on the CMI claims.¹⁷¹⁹

On appeal, the Eleventh Circuit affirmed. The court noted that, while an author’s name can constitute CMI, not every mention of the name does. Here, “Fischer’s” was part of a product name, not a reference to “James H. Fischer” as the owner of a copyrighted text. The court acknowledged that “Natural Honey Harvester” was designed as a closely resembling alternative to “Fischer’s Bee-Quick” and that the advertising copy used on the defendant’s web site and catalog for Natural Honey Harvester mirrored the advertising copy that had been used for Fischer’s Bee-Quick. However, what was removed was not Fischer’s name as the copyright holder of the advertising text, but “Fischer’s” insofar as it was a part of the actual product’s name. In addition, “Fischer’s Bee-Quick used in material published by a third party like the defendant, which contained advertisements for dozens of other products from many different suppliers, could not reasonably be construed as an identifier of the copyright holder of the advertising text. In other words, “Fischer’s” in “Fischer’s Bee-Quick was not used for “managing” copyright information with respect to the text at issue. “Fisher’s” in this context could therefore not be construed as CMI with respect to the advertising text at issue, and the court affirmed the judgment for the defendant.¹⁷²⁰

u. Philpot v. Alternet Media

The plaintiff Larry Philpot was a photographer whose work focused exclusively on concert events across the United States. The defendant operated an alternative news web site and companion Facebook page where it published and posted original content as well as content from other sources. Philpot owned a photo of Willie Nelson, which he made available through Wikimedia pursuant to the terms of the Creative Commons Attribution 2.0 Generic license. On the Wikimedia web site and Philpot’s personal web site, the photo of Willie Nelson contained CMI and metadata indicating that Philpot was the author of the photo, the photo must be attributed to him, and the photo was copyrighted by him. Philpot alleged that the defendant

¹⁷¹⁸ Id. at 610-11.

¹⁷¹⁹ Id. at 611, 619.

¹⁷²⁰ Fischer v. Forrest, 968 F.3d 216, 223-24 (11th Cir. 2020), cert. denied, 142 S. Ct. 460 (2021).

violated Section 1202 by posting his photo with a superimposed quote on the defendant's Facebook page without permission from or attribution to Philpot.¹⁷²¹

The court granted the defendant's motion to dismiss the CMI claim for failure to establish the required mental state for a violation of Section 1202. Philpot argued that his complaint sufficiently pled the defendant's mental state by stating that the defendant should have known its alleged removal of the CMI on the Willie Nelson photo would induce, enable, facilitate, or conceal an infringement of his rights. The court found this argument to be merely conclusory and noted that the complaint contained no factual allegations sufficient to raise a right to relief above the speculative level.¹⁷²²

v. Design Basics v. Ashford Homes

In this case the plaintiffs asserted that the defendants copied and built homes using their copyrighted home designs and brought claims for copyright infringement and false CMI on the defendant's allegedly copied designs. The court denied the defendant's summary judgement motion on the copyright claims, finding disputed issues of fact concerning whether the defendants had access to the copyrighted designs and whether the defendants' design plans were substantially similar to the plaintiffs' design plans.¹⁷²³

With respect to the Section 1202 claim, the court noted that demonstrating copyright infringement does not in and of itself prove that a defendant removed CMI from a work. Copying or re-drawing virtually identical designs, but not including the original CMI, is not the same as altering or removing the CMI from the original design.¹⁷²⁴ The court refused to grant summary judgment on the CMI claim based on the following rationale:

A plaintiff cannot prove a violation of the DMCA without first proving the ownership and access elements of a copyright infringement claim. The Court has concluded that Plaintiffs have established ownership of valid copyrights as a matter of law, but that genuine disputes of material fact remain on the issue of whether [the defendants] had access to the Copyrighted Works. Further, Plaintiffs submitted evidence, without contradiction, that all of their home design plans advertised on the internet and in plan catalogs, including the Copyrighted Works, features their CMI. The allegedly infringing home design plans offered by [the defendants] display [the defendants'] CMI, not Plaintiffs' CMI. The Court concluded above that genuine issues of material fact are disputed as to whether the [defendants'] plan designs are substantially similar to the Copyrighted Works. Genuine issues of material fact likewise are in dispute as to whether

¹⁷²¹ Philpot v. Altnet Media, Inc., 2018 U.S. Dist. LEXIS 203500 at *1-3 (N.D. Cal. Nov. 30, 2018).

¹⁷²² Id. at *13-14.

¹⁷²³ Design Basics, LLC v. Ashford Homes, LLC, 2018 U.S. Dist. LEXIS 212442 at *1, *26 & *47-48 (S.D. Ohio Dec. 18, 2018).

¹⁷²⁴ Id. at *50.

[the defendants] violated the DMCA by removing or changing the Plaintiffs' CMI on the design plans.¹⁷²⁵

w. Design Basics v. WK Olson Architects

The plaintiffs were architectural design companies that created and licensed home plans. They discovered home plans on the defendants' web sites that appeared to copy those of the plaintiffs and brought claims for copyright infringement and claims under Section 1202 for removing or omitting the plaintiffs' CMI from the allegedly infringing plans. The court dismissed the CMI claims, noting that an action for removal of CMI requires that the information was removed from the plaintiff's product or original work. Here, the plaintiffs did not allege that the defendants directly reproduced the plaintiffs' plans without CMI. Instead, they alleged that the defendants' copied aspects of their original works and created virtually identical plans. The court noted that basing a drawing on another's work is not the same as removing CMI from copies of that other work. Virtually identical plans could have been created by redrawing the copyrighted plans in an infringing way and not including the plaintiffs' CMI. Accordingly, the court dismissed the Section 1202 claim.¹⁷²⁶

x. FurnitureDealer.net v. Amazon

FurnitureDealer.Net (FDN), a furniture marketing company, contracted with Coaster Company of America (Coaster) to create a web site to market the products of Coaster. The contract between the parties provided that FDN would own the web site but license it to Coaster. FDN created the web site, including search engine optimization (SEO) text to market Coaster's products, using Coaster's catalog as a starting point. To alert third parties against using copyrighted material, FDN placed a graphic on each page of the web site, which included FDN's logo and a statement saying, "All rights reserved. Nothing on this page may be copied or reproduced without explicit permission." FDN learned that Coaster was providing copyrighted material it created for Coaster, including the SEO text, to Amazon.com and that the SEO text was appearing on Amazon URLs used to promote and sell Coaster furniture. FDN brought suit for copyright infringement against Amazon and Coaster and for removal of FDN's CMI. Coaster moved to dismiss under Rule 12(b)(6).¹⁷²⁷

Coaster argued that the SEO text was not copyrightable subject matter under the merger doctrine because the search engine optimization process used in the creation of the SEO text limited the number of ways the ideas behind the text could be expressed. The court disagreed, noting that while the language FDN used in writing the furniture descriptions was influenced by the SEO process, the ideas behind those descriptions could nonetheless be expressed in a variety of ways. FDN had explained that its process was fairly involved, such that the authors, not an

¹⁷²⁵ Id. at 50-51 (citations omitted).

¹⁷²⁶ Design Basics, LLC v. WK Olson Architects, Inc., 2019 U.S. Dist. LEXIS 21873 at *1-2, *16 (N.D. Ill. Feb. 11, 2019).s

¹⁷²⁷ FurnitureDealer.net, Inc. v. Amazon.com, Inc., 2019 U.S. Dist. LEXIS 41580 at *1-2, *4-5 (D. Minn. Mar. 14, 2019).

algorithm, ultimately determined how their marketing ideas would be expressed. The court also rejected Coaster's argument that the SEO text was not copyrightable under the words and short phrases doctrine. The court noted that the SEO text consisted of more than single words, short phrases, labeling, or technical descriptions, and included unique phrasing and language that seemed designed to maximize the attractiveness of the products described to online buyers.¹⁷²⁸

Coaster further argued that it was a joint author and therefore a joint owner of the copyright in the web site and, as such, it shared equal rights with FDN to any content on the site. The court noted a split of authority with respect to the intent that joint authors must share in order for a joint work to be created. One view is that the parties need only intend to integrate their contributions into a unitary whole. Another view, shared by the Second and Seventh Circuits, is that joint authors must intend at the time they make their contributions to regard themselves as joint authors. The court adopted the view of the Second and Seventh Circuits. The court therefore asked whether Coaster was a joint author of either the SEO text or of the web site. The court found that Coaster's provision of its product catalog to FDN as starter text for the product descriptions did not make it a joint author of the SEO text. The provision of short words and phrases to FDN through its catalog did not make Coaster a genuine collaborator nor show the intent necessary for joint authorship. Nor was Coaster's acts of contributing photos and logos, providing product information and discussing ideas with FDN sufficient. It was not clear to the court that Coaster's contributions to the web site were more than de minimis, but even if they were, the court found that the web site was best characterized as a collective, not a joint, work, with each party owning its individual contributions. The contract between the parties provided that Coaster would keep rights to any design elements it contributed to the web site, and that any content created by FDN would belong exclusively to FDN. These provisions suggested that the parties lacked the intent required for joint authorship of the web site.¹⁷²⁹

FDN alleged that the copyright notice it placed on the web site was CMI and that, by sharing the SEO text with Amazon knowing that it would be displayed without the notice, Coaster violated Sections 1202(b)(1) and (b)(3). In defense, Coaster argued that the notice was false or misleading because it asserted that FDN had a copyright on web site when in fact Coaster held that copyright, and because the notice suggested that FDN owned all the material on the web site when some of the material belonged to Coaster. Coaster therefore argued that FDN had not adequately alleged that valid CMI existed for Coaster to remove or alter.¹⁷³⁰

The court noted that, while there might be some merit to Coaster's argument, the court was not prepared to dismiss FDN's DMCA claim on the pleadings because it was not clear from them that Coaster owned a valid copyright in the web site. Nor was it obvious that the notice implied that FDN owned material that rightfully belonged to Coaster. In addition, the court noted that the notice could be valid even if Coaster was correct that it implied FDN owned material that belonged to Coaster. In the case of a collective work, under Section 404(a), a single

¹⁷²⁸ *Id.* at *9-12.

¹⁷²⁹ *Id.* at *15-19.

¹⁷³⁰ *Id.* at *22-24.

notice applicable to the work as a whole is sufficient as applicable with respect to the separate contributions it contains regardless of the ownership of the copyright in the contributions. In other words, said the court, when the owner of a collective work posts CMI, the CMI's protection extends to its individual contributions, even if the rights to those contributions belong to different authors. Thus, if FDN was the owner of the web site – a question which the court was not determining – a blanket notice covering its own contributions and others' would be valid. But the court noted that, because it did not necessarily follow that the owner of a contribution could post CMI for the collective work as a whole, matters could be more complicated if, after discovery, it appeared that Coaster was the owner of the web site. The court concluded that it need not address this issue until the relevant factual questions had been answered. The court therefore denied Coaster's motion to dismiss the DMCA claim.¹⁷³¹

y. GC2 v. Int'l Game Tech.

In this case, the court ruled that the prohibitions of Section 1202(b) can apply to collaborative or derivative works not solely created by the plaintiff and that failure to affix CMI to copies of a product as contractually required can violate Section 1201(b). GC2 licensed the defendant to use in its games artwork developed by GC2. GC2 alleged that the defendants removed or altered GC's CMI from the artwork during development of the games and then distributed the artwork knowing that the information had been removed. A jury found in favor of GC2 on its Section 1202(b) claim. The defendants contended in a post-trial motion that, because the artwork used in the disputed online versions of its game was the result of a collaborative process, in which modifications were made to create a derivative work, it was not GC2's "original work" and removal of CMI was therefore not a violation.¹⁷³² The court noted that this argument amounted, in effect, to a contention that the statute simply cannot apply to collaborative or derivative works. The court rejected this argument as founded only on language from some district court decisions that does not even appear in the statute, and those decisions were distinguishable in any event.¹⁷³³

The court also rejected the defendants' argument based on the fact that GC2 had not placed CMI on the artwork in the games, but rather had merely supplied the artwork on a CD that did not bear CMI. Because it was the defendants who then placed GC2's logo on the artwork on the physical game machines the companies collaboratively developed, as required by contract, the defendants argued that such logo was not preexisting on the artwork GC2 supplied to the defendants and GC2 could not therefore claim that the defendants removed that information. The court rejected this argument based on the reasoning from the Monotype Imaging v. Bitstream case (discussed in Section II.G.1(b)(2)(i)d above), which held that although the defendant had not literally "removed" copyright notices but instead made copies of the disputed materials without including the copyright notice, this did not preclude liability under

¹⁷³¹ Id. at *23-26.

¹⁷³² GC2 Inv. V. Int'l Game Tech., 391 F. Supp. 3d 828, 837 & 843 (N.D. Ill. 2019) (quoting Monotype Imaging, Inc. v. Bitstream Inc., 376 F. Supp. 2d 877, 893 (N.D. Ill. 2005)).

¹⁷³³ Id. at 843.

the DMCA. The court noted that here, as in Monotype, the defendants could not hide behind an unreasonably crabbed reading of the word “remove.” Nowhere does the text of Section 1202 suggest that removal of CMI is a violation only if that information was placed on the copyrighted materials by the plaintiff itself.¹⁷³⁴ “Such a reading would lead to the absurd result where a copyright owner who contracts with another entity to manufacture their products – and in the process to affix copyright management information – could not avail itself of the DMCA’s removal provisions. The Court declines to adopt the defendants’ requested approach.”¹⁷³⁵

z. Soos & Associates v. Five Guys Enterprises

This case is discussed in Section II.G.1(b)(2)(ii)(j) below.

aa. Dominick R. Pilla v. Gilat

The plaintiff provided professional architectural services to various construction projects. It created two sets of architectural drawings that it alleged the defendants copied without approval and submitted to the New York City Department of Buildings (DOB). The plaintiff brought a claim under Section 1202(b), which the defendants sought to dismiss on the ground that the plaintiff’s allegations were conclusory and failed to allege that the defendants submitted plans with CMI removed, did not detail when, how or where the CMI was removed, and did not provide an example of an allegedly infringing design. The defendants also argued that because they had established that their designs were not exact copies of the plaintiff’s designs with the CMI removed, the plaintiff could not state a claim under the DMCA.¹⁷³⁶

The court found that at this early stage of the litigation, and drawing all inferences in favor of the plaintiff, the plaintiff had stated a claim for removal of CMI, albeit barely. First, the plaintiff alleged the existence of CMI on its designs. The designs attached to the complaint included the plaintiff’s logo, name, and seal, as well as a note stating that the entire contents of the document and all copyrights therein were the sole and exclusive property of the plaintiff and could not be used, photocopied, or reproduced digitally, electronically or in any other manner without the express written consent of the plaintiff. The plaintiff further alleged that the defendants had intentionally removed its CMI from the designs. Although the plaintiff did not allege how, when, or where this removal occurred, such details were not required at the pleading stage for a claim under the DMCA. The plaintiff had also pleaded that the defendants copied the plaintiff’s designs without authorization or approval and submitted certain derivative

¹⁷³⁴ Id. at 844-45.

¹⁷³⁵ Id. at 845. The court also upheld the jury’s awarding of statutory damages based on both original uploads of the game without the required CMI, as well as reuploads of the game, to servers accessible by game users. In addition, the court found that the evidence supported the jury’s conclusion that each reupload constituted three separate violations because three separate versions of the copyrighted works found to have had removed or altered CMI were uploaded. Id. at 850.

¹⁷³⁶ Dominick R. Pilla, Architecture-Eng’g P.C. v. Gilat, 2020 U.S. Dist. LEXIS 48190 at *1-2, *37 (S.D.N.Y. Mar. 19, 2020).

designs to the DOB. Drawing all inferences in favor of the plaintiff, the court concluded that the plaintiff plausibly alleged that the CMI was removed at the time of the unlawful copying.¹⁷³⁷

The court also concluded that, although sparse, the plaintiff alleged sufficient facts to suggest that the defendants acted intentionally. For example, the complaint alleged the defendants were aware at all times of the plaintiff's copyrights, had access to the plaintiff's designs, copied the designs and submitted derivative designs, and "may have used, distributed, marketed, and displayed ... [the plaintiff's designs] for other construction projects."¹⁷³⁸ Taken together, the court found these allegations sufficient to give rise to a plausible inference that the defendants were aware of the appropriate uses of the plaintiff's CMI and, in allegedly copying the designs, intentionally altered or removed the plaintiff's CMI. In addition, although the defendants argued they had established that their designs were not exact copies of the plaintiff's, thus precluding a claim under the DMCA that CMI was altered or removed, the court held that this argument was better reserved for summary judgment, when there was a fully developed record. The court therefore denied the defendants' motion to dismiss the DMCA claims.¹⁷³⁹

bb. Philips N. Am. v. Summit Imaging

The plaintiff Philips manufactured and sold ultrasound imaging devices that included certain software and hardware features that could be used only when Philips enabled a particular licensable feature for the specific ultrasound system based on what features a customer had purchased. Philips alleged that the defendant hacked into Philips' software and altered the ultrasound systems using a computer program it developed called Adepto so as to enable features or options for which Philips' customers had not paid. Among other things, Philips brought claims under Sections 1202(a) and (b). The defendants moved to dismiss the CMI claims.¹⁷⁴⁰

The court found that Philips had failed to plead a plausible claim for relief under Section 1202. The only CMI identified with any specificity in the complaint was the terms and conditions of the use of the software, which Philips alleged resided on machine readable configuration files. Although terms and conditions qualify as CMI under Section 1202(c), the court found that Philips offered no details explaining how the defendants falsified, removed, or altered Philips' terms and conditions. Instead, Philips included only boilerplate allegations that the defendants' business of modifying Philips' ultrasound systems included modifications to such CMI. Without factual detail to explain what modifications the defendants made to the terms and conditions, how the defendants made those modifications, or the method by which they distributed this modified CMI, the court ruled that the complaint offered only naked assertions that were insufficient to

¹⁷³⁷ Id. at *37-39.

¹⁷³⁸ Id. at *39.

¹⁷³⁹ Id. at *40-41.

¹⁷⁴⁰ Philips N. Am., LLC v. Summit Imaging Inc., 2020 U.S. Dist. LEXIS 55073 at *1-3, *11 (W.D. Wa. Mar. 30, 2020).

survive a motion to dismiss. The court, however, granted Philips leave to amend the CMI claim.¹⁷⁴¹

cc. Bell v. Worthington City Sch. Dist.

The plaintiff argued that the defendant violated Section 1202(b) by retweeting a tweet posted on another entity's Twitter account that included a passage from the plaintiff's book, with the plaintiff's name removed from the passage. The defendant argued that no violation of Section 1202(b) occurred because at the time of the retweet, only the book containing the passage was copyrighted, not the passage itself, and there was no CMI for the book on the pages of the book where the passage appeared. The court agreed, pointing to several district court decisions holding that when a part of a copyrighted work is used, a defendant cannot be liable under Section 1202(b) unless it removed CMI from the part of the work it copied, or close to the part of the work copied. Although the court noted one district court decision rejected this rule and instead holding that to prove a cause of action under Section 1202(b) the defendant need only show that the piece of the work used was obtained from a source which contained CMI, the court in this case chose to follow the majority of cases. The court noted the plaintiff had not provided any evidence that there was any CMI on or near the passage of his book that was retweeted. And even if it were to assume that the plaintiff's book included CMI at the bottom of each page, the court found the plaintiff has provided no argument or evidence that the person who made the retweet intentionally removed this information. Accordingly, the court granted the defendant summary judgment on the plaintiff's Section 1202 claim.¹⁷⁴²

dd. RAZ Imports v. Regency Int'l Bus. Corp.

The plaintiff was the designer of a sculpture titled "Marshmallow Spray." The defendant created a sculpture that was substantially similar to the plaintiff's sculpture. The plaintiff brought claims for copyright infringement and violation of Sections 1202(a) and (b). The plaintiff alleged that the "Marshmallow Spray" title and the plaintiff's identity as the author, owner or source constituted CMI. With respect to Section 1202(a), the plaintiff alleged that the defendant provided false CMI on its own product by claiming a substantially similar product as its own. The court rejected this argument, ruling that, because the plaintiff complained of false CMI presented in connection with products generated by the defendant, as opposed to the RAZ Marshmallow Spray product itself, the plaintiff had not stated facts to support a claim for a violation of Section 1202(a).¹⁷⁴³

The plaintiff asserted violations of Section 1202(b) based on the defendant's altering the title of the copyrighted work to "Marshmellow Spray" and removing any indication the plaintiff was the author, owner, or source of the work. The court noted that one district court decision had previously noted the possibility of a divide developing between courts concluding Section

¹⁷⁴¹ Id. at *13-14.

¹⁷⁴² Bell v. Worthington City Sch. Dist., 2020 U.S. Dist. LEXIS 96424 at *3-7, *37-42 (S.D. Ohio June 2, 2020).

¹⁷⁴³ RAZ Imports, Inc. v. Regency Int'l Bus. Corp., 2020 U.S. Dist. LEXIS 139406 at *2, *7-8 (N.D. Tex. Aug. 5, 2020).

1202(b) requires a showing that CMI was removed from the plaintiff's work itself, and those allowing a claim to proceed with allegations that CMI was "created anew" on the defendant's infringing work.¹⁷⁴⁴ Although the court expressed doubt about whether such a divide was in fact occurring, the court ruled that failure to place the plaintiff's CMI on an allegedly infringing new product that is substantially similar to the plaintiff's product (here, the failure to identify images of the defendant's allegedly infringing products on its web site as the plaintiff's Marshmallow Spray authored and owned by the plaintiff), as opposed to removing CMI from copies of the plaintiff's product, did not state a claim under Section 1202(b). Accordingly, the court dismissed the plaintiff's Section 1202(a) and (b) claims.¹⁷⁴⁵

ee. Neo4j v. Graph Foundation

The plaintiff Neo4j offered a free version of a graph database computer program known as the Neo4j Community Edition under the open source GNU General Public License (GPL), and a more advanced commercial version of the software known as the Neo4j Enterprise Edition, which initially was offered under a proprietary commercial license and under a more restrictive version of the GPL known as the GNU Affero General Public License version 3 (AGPL v3). In May 2018, Neo4j Sweden replaced the AGPL v3 with a stricter license, the Neo4j Sweden Software License, which included the terms of the AGPL v3 with additional restrictions known as the "Commons Clause." In November 2018 Neo4j ceased offering the Neo4j Enterprise Edition under any open source license, instead offering it only under a proprietary commercial license. In June 2018, in response to Neo4j's announced decision to cease offering the Neo4j Enterprise Edition on an open source basis, the defendant Graph Foundation, Inc. (GFI) was organized as a nonprofit organization to offer a graph database software called "ONgDB," which was described as the "free and open source Neo4j Enterprise project" and "a non-restrictive fork of Neo4j, the world's leading Graph Database." GFI also referred to ONgDB as the "Open Neo4j Enterprise project."¹⁷⁴⁶

Neo4j sued GFI under Section 1202(b) for unauthorized alteration of its CMI on the Neo4j Enterprise Edition, which GFI alleged included the owner's name, a copyright notice, and a license providing the terms and conditions for use of the copyrighted work in a LICENSE.txt file. Neo4j asserted GFI violated Section 1202(b) by intentionally distributing altered Neo4j source code knowing that the CMI in that source code had been removed. GFI argued that Section 7 of the AGPL v3 prohibited licensors like Neo4j Sweden from adding restrictions beyond those set out in the form AGPL v3 and that the Commons Clause included in the Neo4j Sweden Software License was a "further restriction" under the terms of the form AGPL v3 and could be properly removed by a licensee in the licensee's distributions of the source code. The court construed various relevant provisions of the Neo4j Sweden Software License to conclude that it did not permit the alleged removal or alteration of CMI in the Neo4j Enterprise Edition source code. The

¹⁷⁴⁴ *Id.* at *7, *10 (citing Aaberg v. Francesca's Collections, Inc., 2018 U.S. Dist. LEXIS 50778 at *8 (S.D.N.Y. Mar. 27, 2018)).

¹⁷⁴⁵ RAZ Imports, 2020 U.S. Dist. LEXIS 139406 at *10-11.

¹⁷⁴⁶ Neo4j, Inc. v. Graph Foundation, Inc., 2020 U.S. Dist. LEXIS 212896 at *2-5 (N.D. Cal. Nov. 13, 2020).

court noted that Section 10 of the AGPL v3, which was incorporated into the Neo4j Sweden Software license, stated: “You may not impose any further restrictions on the exercise of rights granted or affirmed under this License.” Section 7 stated, “If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term.” GFI argued that these provisions meant that there could be no liability for removing the further license restriction which Neo4j Sweden incorporated into the license, namely the Commons Clause. The court noted, however, that the AGPL v3 defines “you” as the licensee, not the licensor. Thus, read correctly, Sections 7 and 10 prohibited a *licensee* from imposing further restrictions, but did not prohibit a *licensor* from doing so. The court therefore ruled that the terms drawn from the APGL v3, on which the Neo4j Sweden Software License was based, did not limit the rights of Neo4j Sweden to include the Commons Clause or any other additional restriction in its own copyright license.¹⁷⁴⁷

GFI further argued that Neo4j’s knowledge allegations were too conclusory to support a Section 1202(b) claim. The court rejected this argument, noting that Neo4j had alleged that GFI knowingly copied source code from the Neo4j Software License, stripped out the CMI governing the source code, published the altered files on its Github repository for ONgDB, then advertised ONgDB as a free and open source Neo4j Enterprise project and a non-restrictive fork of Neo4j. The court ruled that, drawing all inferences in favor of Neo4j, these allegations plausibly suggested that GFI distributed Neo4j Enterprise Edition source code in which the CMI was removed or modified with the specific intent of providing an open source, restriction-free version of the software in violation of the Neo4j Sweden Software License. In addition, given that the Neo4j Sweden Software License prohibited third parties from offering support services, and Neo4j had alleged that GFI marketed ONgDB in order to profit off of support and development services, it was reasonable to conclude that GFI acted with knowledge that its actions would induce, enable, facilitate, or conceal infringement.¹⁷⁴⁸

Finally, the court rejected GFI’s argument that its removal of CMI from the Neo4j Sweden Software License did not violate Section 1202(b) because the CMI was not removed entirely, but instead was moved to separate text files (the NOTICE.txt files). GFI asserted that, other than the Commons Clause language itself, all of the language removed from the Neo4j Sweden Software License from the LICENSE.txt file was included in the NOTICE.txt file for each of the source code files copied from Neo4j Enterprise Edition along with the copyright attribution language. The court noted that the NOTICE.txt files were not referenced in the complaint and it declined to exercise judicial notice over the documents merely because they were found on the same web site as exhibits that were attached to the complaint. In any event, the court noted that Section 1202(b) prohibits distributing a work knowing that CMI has been removed or altered. The court ruled that moving the CMI into separate NOTICE.txt files constituted altering the CMI, and conveying the Neo4j Sweden Software License without the Commons Clause constituted removing CMI. Thus, the fact that GFI conveyed most of the removed CMI in NOTICE.txt files did

¹⁷⁴⁷ *Id.* at *8-12.

¹⁷⁴⁸ *Id.* at *12-14.

not insulate it from potential liability under Section 1202(b). The court therefore denied GFI's motion to dismiss the Section 1202(b) claim.¹⁷⁴⁹

ff. Munro v. Fairchild Tropical Botanic Garden

The plaintiffs owned copyright in an outdoor light sculpture called "Forest of Light" and alleged that the outdoor displays of defendants' "mushroom" exhibit and "fiber light" exhibit constituted copyright infringement. The plaintiffs also brought claims under Sections 1202(a) and 1202(b) for false or altered CMI based on (1) defendants' preparing and distributing a pitch deck, website and social media that contained photos of their outdoor exhibits, which plaintiffs alleged were copies of their works without authorization and attribution, and (2) publicly displaying their exhibits outdoors without CMI and showing guide maps and signage with false/alterd CMI instead of the plaintiffs' CMI.¹⁷⁵⁰

The court granted summary judgment to the defendants on all CMI claims. Although the court agreed with the plaintiffs that CMI need only be conveyed "in connection with" copies of a work and need not be affixed to the actual body of the work, where CMI has not been affirmatively removed from a plaintiff's original work, but instead some of the work's elements are merely copied into a different form compiled by the defendant, there is no CMI violation under Section 1202(b). Here, it was undisputed that the plaintiffs did not create the allegedly infringing mushroom and fiber light exhibits or the photos contained on the webpage, the guide map, or the pitch deck. And the undisputed evidence showed that the defendants found the photos through a Google search, and there was no evidence that any defendant removed or altered CMI from the images found on Google, much less that any defendant acted with the double scienter requirement of Section 1202(a). Accordingly, the plaintiffs could not establish that the defendants knowingly and with the intent to enable infringement provided or distributed false CMI with respect to those materials. And even if the pitch deck images were considered copies of the plaintiffs' work under Section 1202(b)(3) and were distributed, there again was no evidence that the defendants knew that CMI was removed or altered without the plaintiffs' authority.¹⁷⁵¹

(ii) Cases re False CMI

a. Schiffer Publishing, Ltd. v. Chronicle Books, LLC

In Schiffer Publishing, Ltd. v. Chronicle Books, LLC,¹⁷⁵² the plaintiffs owned copyrights in various photographs of fabrics, which the defendants allegedly infringed by scanning into digital form for inclusion into a book published by the defendants titled *1000 Fabrics*. The plaintiffs also

¹⁷⁴⁹ Id. at *14-16.

¹⁷⁵⁰ Munro v. Fairchild Tropical Botanic Garden, 2022 U.S. Dist. LEXIS 27504 at *2-3, *6 & *26 (S.D. Fla. Jan. 13, 2022).

¹⁷⁵¹ Id. at *25-30.

¹⁷⁵² 73 U.S.P.Q.2d 1090 (E.D. Pa. 2004).

alleged that the defendants had violated Sections 1202(a) and (b) by falsely naming themselves as the copyright holders of the pictures published in *1000 Patterns* and by “removing” the plaintiffs’ copyright notices from those pictures.¹⁷⁵³

The court found no violation of the CMI provisions of the DMCA. The court noted that to recover for a violation of Section 1202(a), a plaintiff must prove that the defendant knew the CMI on a distributed work was false and distributed the false CMI with the intent to aid infringement. The court ruled that the plaintiffs had not shown that the defendants possessed the requisite knowledge or intent to violate the relevant copyrights. Although there was evidence at trial that the defendants instructed its employees to avoid using too many series of page images from any single book containing the plaintiffs’ photographs, the court found the evidence indicated only that the defendants knew the plaintiffs had copyrights in their books as compilations, not that they knew the individual photographs contained therein were copyright protected. Other evidence at trial suggested that the defendants erroneously believed the plaintiffs had no copyright in their individual photographs because they contained insufficient creativity. Accordingly, the intent requirement of Section 1202(a) was not met.¹⁷⁵⁴

The court also found no violation of Section 1201(b) because the only CMI the plaintiffs included with their work were notices of copyright that appeared on the inside covers of their books. The individual photographs that were the subject of the action did not contain any CMI whatsoever, either on or near the images themselves. The court ruled that to establish a violation of Section 1202(b), the defendants must remove CMI from the body of, or area around, the plaintiffs’ work. Because the plaintiffs had failed to demonstrate the defendants had done so, the claim for violation of Section 1202(b) failed.¹⁷⁵⁵

b. Agence France Presse v. Morel

The facts of this case are set forth in Section II.G.1(b)(1)(ii) above. In ruling on the motion of Agence France Presse (AFP) to dismiss the claim against it for falsification of CMI, the court found Morel’s allegations that AFP labeled his photos with the credit lines “AFP/Getty/Daniel Morel” and “AFP/Getty/Lisandro Suero” to be sufficient to plead falsification of CMI. AFP had not contested that those credit lines constituted CMI. Morel also set forth a factual basis for alleging that AFP knew the CMI was false and intended to facilitate infringement. Morel alleged that an AFP photo editor viewed his photos before asking about identical photos on Suero’s TwitPic page, and that when Morel failed to respond to the editor’s email, AFP downloaded the pictures from Suero. Morel further alleged that AFP knew the photos were his because he was a well-known photographer and AFP had no reason to believe Suero took the photos. However, AFP credited Suero without inquiry. As to Getty, Morel alleged that even after AFP issued a wire to change the photographer credit from Suero to Morel, Getty continued to license photos crediting Suero. Getty sought to obtain credit for the photographs even though it knew of

¹⁷⁵³ Id. at 1101.

¹⁷⁵⁴ Id. at 1102.

¹⁷⁵⁵ Id.

Morel's reputation and had not investigated Suero's authorship. The court concluded that these allegations sufficiently plead knowledge and intent.¹⁷⁵⁶

After discovery, the parties cross-moved for summary judgment on the CMI claims. The court denied the motions based on various factual disputes,¹⁷⁵⁷ for the reasons summarized in Section II.G.1(b)(1)(ii).e above. In a subsequent opinion, discussed in Section III.C.6(b)(1)(iii).v below, the court determined that both AFP and Getty were direct infringers for the distribution of unauthorized copies of Morel's photos and allowed the case to go to a jury on the copyright infringement claims and the CMI claims. In Nov. 2013, a New York federal jury found that both AFP and Getty had willfully infringed Morel's copyright in the eight photographs, awarded Morel \$275,000 in actual damages, \$28,889.77 total in infringer's profits, and \$1.2 million in statutory damages; found that AFP and Getty had jointly committed sixteen violations of the CMI provisions of the DMCA for the distribution of false bylines; and awarded Morel an additional \$20,000 for those DMCA violations. Morel elected to receive statutory damages in lieu of actual damages and infringer's profits, and the court entered judgment in the total amount of \$1,220,000. As discussed in greater detail in Section III.C.6(b)(1)(iii).v below, the defendants' subsequent motions for JMOL, new trial and/or remittitur were denied, except Getty's motion for JMOL with respect to Section 1202(b) liability was granted. AFP and Getty remained jointly liable for \$1.2 million in statutory damages, and AFP was held individually liable for \$10,000 of statutory damages under the CMI provisions of the DMCA (one half of the total the jury awarded against AFP and Getty).¹⁷⁵⁸

c. Personal Keepsakes v. PersonalizationMall.com

This case is discussed in Section II.G.1(b)(2)(i).k above.

d. Drauglis v. Kappa Map Group

The plaintiff in this case was the owner of the copyright in a photograph that he posted on a web site under the Creative Commons license CC BY SA 2.0. The defendant obtained a copy of the photograph and placed it on the front cover of its atlas. The court, rejecting the plaintiff's arguments to the contrary, found that the defendant had complied with all of the provisions of the Creative Commons license in its utilization of the photograph on the atlas. The plaintiff also asserted that a copyright notice on the first inside page of the atlas in the name of the defendant constituted false CMI with respect to the photograph because it incorrectly implied that the defendant owned the copyright to the photograph. The defendant moved for summary judgment on the CMI claim.¹⁷⁵⁹

¹⁷⁵⁶ Agence France Presse v. Morel, 769 F. Supp. 2d 295, 304-05 (S.D.N.Y. Jan. 14, 2011).

¹⁷⁵⁷ Agence France Presse v. Morel, 934 F. Supp. 2d 547, 574-78 (S.D.N.Y. 2013).

¹⁷⁵⁸ Agence France Presse v. Morel, 2014 U.S. Dist. LEXIS 112436 at *6-7, *10-29 (S.D.N.Y. Aug. 13, 2014).

¹⁷⁵⁹ Drauglis v. Kappa Map Group, LLC, 128 F. Supp. 3d 46, 52-59 (D.D.C. 2015).

The court rejected the plaintiff's claim for false CMI. First, the court noted that just because a notice may qualify as a copyright notice under Section 401 of the copyright statute does not mean that it automatically constitutes CMI as defined in Section 1202. The definition of CMI in Section 1202 requires that information be "conveyed in connection with" copies of a work. Generally, to satisfy that requirement, the information must be close to the work. The court concluded that, because the copyright notice on the first inside page of the atlas was not in the body of, or the area around, the photograph, it was not conveyed in connection with the cover photograph in a way that made it CMI. Because the copyright notice was not CMI with respect to the photograph, the court decided it need not reach the plaintiff's allegation that the defendant knew its notice was false or that it intended to provide false information in order to enable copyright infringement. Accordingly, the court granted the defendant summary judgment on the false CMI claim.¹⁷⁶⁰

e. Stevens v. CoreLogic

(The facts of this case and the court's rulings with respect to false CMI are set forth in Section II.G.1(b)(2)(i).n above.)

f. GC2 v. Int'l Game Tech.

In GC2 Inc. v. Int'l Game Tech. PLC,¹⁷⁶¹ the plaintiff owned copyrights in artwork primarily displayed on physical wagering machines such as slot machines. The plaintiff brought a copyright infringement claim against the defendant International Game Technology PLC (IGT) for the unauthorized sale of online games containing its artwork, which IGT offered through the web site of its wholly owned subsidiary, DoubleDown. The plaintiff also asserted a claim for false CMI under Section 1202(a), which IGT sought to dismiss under Fed. R. Civ. Pro. 12(b)(6).¹⁷⁶² The false CMI claim was based on the fact that DoubleDown's terms of use for its web site stated that DoubleDown "and/or its licensors and affiliates own all right ... copyrights ... and other intellectual property rights" on its web site, including rights to the "graphics, texts, information, pictures, video" displayed.¹⁷⁶³

The court ruled the plaintiff had adequately alleged that the terms of use contained false statements in that DoubleDown did not own or have a license to display the plaintiff's copyrighted materials and yet did so on its web site. The court determined, however, that the plaintiff had failed to adequately allege that the false statements in the terms of use were "conveyed in connection with" the plaintiff's artwork, as required by Section 1202(c). The plaintiff contended that DoubleDown's terms of use were conveyed in connection with the artwork because every page of the web site containing the plaintiff's artwork had a link at the bottom of the page or in a dropdown menu to DoubleDown's terms of use agreement. The

¹⁷⁶⁰ Id. at 59-61.

¹⁷⁶¹ 255 F. Supp. 3d 812 (N.D. Ill. 2017).

¹⁷⁶² Id. at 815-16, 821.

¹⁷⁶³ Id. at 821.

court rejected this, noting that courts in previous decisions had generally required more than a boilerplate terms of use notice near a copyrighted work in order to find a party liable for distributing false CMI. Because DoubleDown's terms of use link simply appeared at the bottom of every page on its web site, the plaintiff could not properly allege that the false statements in DoubleDown's terms of use agreement were conveyed in connection with the plaintiff's copyrighted works.¹⁷⁶⁴

The plaintiff further argued that IGT was liable for distributing false CMI because DoubleDown displayed the plaintiff's artwork without showing its trademark, instead including either IGT's own logo and trademark on the artwork or not including any indication of ownership. The plaintiff contended that IGT's omission of the plaintiff's trademark constituted altering or removing CMI. In response, IGT argued that the plaintiff's trademark information on its artwork did not constitute CMI as contemplated by the DMCA. The court rejected this, noting that nothing in Section 1202 requires copyright owners to convey their ownership by way of a copyright notice. Thus, trademark information may constitute CMI if it is used to signal authorship of a copyrighted work, as it was here.¹⁷⁶⁵

IGT also contended that the DMCA was meant to impose liability only where CMI is affirmatively removed or altered from copyrighted works, not where CMI is simply omitted. The court found this contention contrary to the admittedly limited case law on the matter, which indicated that there is liability where a party intentionally omits CMI or facilitates the omission of CMI.¹⁷⁶⁶ Finally, IGT contended that, even if an omission of authorship is actionable under the DMCA, the plaintiff could not show that DoubleDown or other defendants related to IGT intentionally omitted the plaintiff's trademark. The court ruled that this argument was forfeited for purposes of the present motion to dismiss because it was not made in IGT's opening brief but rather was asserted for the first time in its reply. Accordingly, the court denied IGT's motion to dismiss the plaintiff's Section 1202 claim, but stated that the claim would be limited in accordance with the discussion of the claim in its opinion.¹⁷⁶⁷

In an interesting ruling with respect to claims for vicarious copyright infringement brought by the plaintiff, the court ruled that the software license agreements some of the defendants had with their end users governing the online games were sufficient to support allegations that the defendants' had the ability to control their end users. Specifically, under the license agreements, the defendants had the authority to terminate the license or to bring a lawsuit where the end user violated the terms of the agreement. The court read these provisions as sufficient, for purposes of denying a motion to dismiss, to support the plaintiff's

¹⁷⁶⁴ Id. at 821-22.

¹⁷⁶⁵ Id. at 822.

¹⁷⁶⁶ Id. The court cited Agence France Presse v. Morel, 769 F. Supp. 2d 295 (S.D.N.Y. 2011), in which the court found that liability could be imposed if a copyrighted work is displayed without reference to authorship even where the original work did not indicate authorship.

¹⁷⁶⁷ GC2, 255 F. Supp. 3d at 823.

allegation that the defendants had the authority to put a stop to the infringing conduct even after a consumer's one-time purchase of the game.¹⁷⁶⁸

g. Pierson v. Infinity Music & Entm't

In this case, the plaintiff owned copyrights in two photos of different musical bands. The defendant operated a web site on which it displayed event pages for concerts booked at the defendant's venues. The plaintiff's two photos appeared on two event pages at the defendant's site without the plaintiff's permission. At the bottom of each event page appeared a copyright notice in the defendant's name and a link to the defendant's Terms of Use. Although the plaintiff did not claim that the defendant had removed or altered any CMI from her photos, she argued that the defendant's copyright notices and Terms of Use links violated Section 1202(a) because they claimed copyright in all content published on the web site, including the plaintiff's photos. The defendant moved for summary judgment, arguing that the information was not "conveyed in connection with" the plaintiff's photos. The defendant also argued that even if the notices were conveyed in connection with the plaintiff's photos, the defendant lacked the requisite intent to induce, enable, facilitate, or conceal infringement.¹⁷⁶⁹

The court noted that the term "conveyed" in Section 1202(c) "is used in its broadest sense and is not meant to require any type of transfer, physical or otherwise, of the information. It merely requires that the information be accessible in conjunction with, or appear with, the work being accessed."¹⁷⁷⁰ The court held that the Terms of Use were conveyed in connection with the photos because a link to the Terms of Use appeared at the bottom of each relevant web page and because the Terms of Use clearly stated that they were intended to cover all content on the web site, which included the plaintiff's photos. The court noted that physical proximity is not the only appropriate measure of whether a copyright notice constitutes CMI. Rather, the notice need only be accessible in conjunction with, or appear with, the work being accessed. In this case, the notice and the Terms of Use were both easily accessible in conjunction with the plaintiff's photos.¹⁷⁷¹

The defendant argued that it lacked the requisite intent because the copyright notice was a standard notice placed indiscriminately at the bottom of each page of the web site and the defendant did not know that the plaintiff held the copyrights in the photos. The plaintiff argued it was immaterial that the defendant did not know the plaintiff held the copyrights because the defendant must have known that it did not itself own the copyrights in the photos. The plaintiff argued that, by failing to include any carve outs on the web site for content owned by third parties, a reasonable jury could find that the defendant specifically intended to induce, enable, facilitate, or conceal infringement. The court agreed with the plaintiff, noting that the Second

¹⁷⁶⁸ Id. at 824-25.

¹⁷⁶⁹ Pierson v. Infinity Music & Entm't, Inc., 300 F. Supp. 3d 390, 391-94 (D. Ct. 2018).

¹⁷⁷⁰ Id. at 394 (quoting Janik v. SMG Media, Inc., 2018 U.S. Dist. LEXIS 4567 at *12 (S.D.N.Y. Jan. 10, 2018) (in turn quoting S. Rep. 105-190 at 35 (1998))).

¹⁷⁷¹ Pierson, 300 F. Supp. 3d at 395-96.

Circuit had repeatedly recognized that intent is always a subjective matter of inference and thus rarely amenable to summary judgment. Accordingly, the court denied the defendant's motion for partial summary judgment.¹⁷⁷²

h. Zuma Press v. Getty Images

Getty offered for licensing on its web site 47,048 images once owned by or exclusively licensed to Zuma. By mistake, Getty credited the images to "Les Walker," not to Zuma or the photographers that Zuma represented because of the following sequence of events. In 2011, Zuma commingled its images with the collection of Les Walker. Getty later purchased rights to Walker's collection of images, known as the "NewSport" collection, and migrated those images to its database. Because the images claimed by Zuma were part of the NewSport collection, and because the metadata associated with those images indicated that NewSport was the licensing agency, Getty migrated the entire NewSport collection, including the Zuma images. Getty's computer script performing the migration did not look at the free-text portion of the images, where Zuma was referenced, but to the metadata that identified "NewSport" as the source of the images. Zuma brought claims against Getty for copyright infringement and under Sections 1202(a) and (b).¹⁷⁷³

The court granted summary judgment to Getty on the Section 1202 claims on the basis that Getty lacked the requisite intent required under Section 1202. The undisputed facts showed that Getty had no knowledge that Zuma's images were commingled with the NewSport collection, Getty utilized an automated process to migrate the NewSport collection and, by that process, appended CMI referring to NewSport and Getty under the reasonable assumption that the images were owned by NewSport and licensed to Getty. There was no evidence that Getty intended to induce or facilitate infringement. The court further ruled that Zuma was estopped from arguing that Getty engaged in unauthorized use or modification of the Zuma images because Zuma had commingled its images with the NewSport collection, knowing that "NewSport" would be labeled as the "source" and licensor of the images. Zuma attempted to retrieve the images, but did not succeed because NewSport did not give its written consent. Unsuccessful at switching the images to its account, and knowing that its images were inextricably mixed with the NewSport collection, Zuma made no further efforts to retrieve its images. Getty therefore reasonably believed, because of Zuma's actions, that it had the rights to use and license all the images acquired from NewSport, including the photographs that Zuma had commingled.¹⁷⁷⁴

¹⁷⁷² Id. at 396-97.

¹⁷⁷³ Zuma Press, Inc. v. Getty Images (US), Inc., 349 F. Supp. 3d 369, 370-71 & 374 (S.D.N.Y. 2018).

¹⁷⁷⁴ Id. at 376. The court denied a subsequent motion by Zuma for reconsideration on the ground that the court overlooked evidence of Getty's intent to induce or facilitate infringement. The court ruled that Zuma had failed to identify any information or controlling law that the court overlooked. Zuma Press, Inc. v. Getty Images (US), Inc., 2019 U.S. Dist. LEXIS 12415 at *6 (S.D.N.Y. Jan. 24, 2019).

On appeal, the Second Circuit summarily affirmed. The court ruled that a reasonable juror could find only that Getty established the existence of a valid license. As the district court concluded, the undisputed facts and the plain language of each of the agreements at issue establish an unbroken chain of authorization from Zuma to Getty. With respect to the Section 1202 claim, the court ruled that no reasonable juror could conclude that Getty knowingly removed or altered the plaintiffs' CMI without authority. As the district court concluded, there was no evidence on which the plaintiffs could rely to establish that Getty had actual knowledge that the images at issue were comingled with the NewSport collection. On the contrary, a reasonable juror could conclude only that Getty did not know about the plaintiffs' purported rights in the images until Zuma contacted Getty on May 4, 2016 to complain that Getty did not have authorization to use the images – i.e., until after Getty had completed the migration process and posted the images to its web site. Getty promptly thereafter removed whatever images it could identify as associated with Zuma from its public-facing web site and launched a full investigation into what had happened. In addition, a reasonable juror could find only that the purported changes to the plaintiffs' CMI resulted not from some intentional act of which Getty was aware but from aberrations and mistakes in the automatic migration process itself, during which Getty process approximately 7,000,000 images. Accordingly, the Second Circuit affirmed the judgment and order of the district court.¹⁷⁷⁵

i. Michael Grecco Prods v. Alamy

The plaintiff licensed several copyrighted photos for display and sublicensing on the defendant's web site. The plaintiff brought this infringement action alleging that the defendant continued to display and offer to license the photos beyond the termination of the parties' license agreement. The plaintiff also alleged a violation of Section 1202(a) on the ground that the defendant placed visible watermarks, such as "Alamy," "alamy," and "a," on the photos in order to conceal its infringement and induce potential customers to believe that the defendant, not the plaintiff, held exclusive rights in them.¹⁷⁷⁶

The defendant brought a motion to dismiss the Section 1202(a) claim on the ground that its alleged placement of watermarks on the copyrighted photos did not constitute the distribution of CMI because the watermarks did not indicate authorship or copyright ownership and thus were not CMI. Rather, the defendant asserted that the watermarks identified the originator of the web site on which the photos appeared. The court disagreed, finding that because a watermarked corporate name or symbol may refer to the author or copyright owner when displayed on a copyrighted work in connection with the marketing of that work for sale or license, such watermarks do constitute CMI under Sections 1202(c)(2)-(3) & (7). Accordingly, the court ruled that the plaintiff had alleged sufficient facts from which the court could plausibly

¹⁷⁷⁵ Zuma Press, Inc. v. Getty Images (US), Inc., 2021 U.S. App. LEXIS 6139 at *1, *3-4, & *7-8 (2d Cir. Mar. 3, 2021).

¹⁷⁷⁶ Michael Grecco Prods.v. Alamy, Inc., 372 F. Supp. 3d 131, 133-34 (E.D.N.Y. 2019).

infer that the watermarks described in the complaint constituted CMI for the purpose of the alleged Section 1202(a) violation.¹⁷⁷⁷

The court also rejected the defendant's challenges to the adequacy of the plaintiff's pleading of the scienter elements of Section 1202(a). Here, the plaintiff alleged that the defendant was informed the term of its license had expired and that the defendant knew the expiration deprived it of the authority to further license and display the copyrighted photos without further permission from the plaintiff. Additionally, the plaintiff alleged that the defendant placed watermarks on the photos in order to facilitate its continued marketing and sale of licenses. The court held that, while the truth of these allegations had to be ascertained at a later stage of litigation, they were sufficient as stated to survive a motion to dismiss.¹⁷⁷⁸

j. Soos & Associates v. Five Guys Enterprises

In this case, the court determined that the plaintiff had adequately pled claims under both Sections 1202(a) and (b). The defendant Five Guys Enterprises hired the plaintiff Soos & Associates to create architectural plans for several restaurant locations. The parties parted ways, and Soos alleged that after they ended their relationship, Five Guys required its outside architects to use templates of architectural plans that Soos created and copyrighted. Soos further alleged that Five Guys removed Soos' CMI from the templates and required its outside architects to place Five Guys' CMI title blocks into the infringing plans using the Soos works.¹⁷⁷⁹

Five Guys moved for judgment on the pleadings on both DMCA claims. The court found the allegations with respect to the Section 1202(b) claim sufficient. Soos alleged that Five Guys and the new architects made some minor changes to its architectural plans, such as changing the page numbers, but heavily used Soos' format, layout, text, illustrations, and taxonomies. Five Guys argued that Soos had failed to identify the particular CMI removed, to allege facts as to how Five Guys removed the CMI, and to plausibly allege intent. Five Guys also argued that basing a drawing off of another's work is not the same as removing CMI. The court rejected these arguments. The complaint stated that Five Guys knew Soos was asserting ownership over several architectural plans, yet continued to use the copyrighted material and removed Soos' CMI title blocks from the plans. Soos had attached several exhibits to its complaint containing the CMI that Five Guys allegedly removed, which the court found to be adequate identification of the CMI. And the court found that Soos had adequately alleged intent – its complaint stated that based on letters Soos sent to Five Guys, Five Guys knew Soos was asserting ownership of the architectural plans and that Five Guys knowingly distributed templates where the CMI had been altered without the authority of Soos.¹⁷⁸⁰ Finally, Soos alleged that Five Guys "attempted to mislead third party architects into believing Five Guys owned the copyrights in the templates

¹⁷⁷⁷ Id. at 137-38.

¹⁷⁷⁸ Id. at 139.

¹⁷⁷⁹ Soos & Associates, Inc. v. Five Guys Enterprises, LLC, 2020 U.S. Dist. LEXIS 37033 at *3-4 (N.D. Ill. Mar. 3, 2020).

¹⁷⁸⁰ Id. at *8-9.

Five Guys demanded they use.”¹⁷⁸¹ The court concluded these allegations were sufficient to survive a motion for judgment on the pleadings as to its Section 1202(b) claim and that Soos was not required to provide detailed factual allegations regarding how Five Guys removed the CMI.¹⁷⁸²

With respect to the Section 1202(a) claim, Soos alleged that it sent several letters to Five Guys claiming ownership of the architectural plans and that, despite these letters, Five Guys continued to copy Soos’ work, removed Soos’ CMI from the plans, and placed false CMI on the plans. Soos also alleged that even though Five Guys knew that Soos claimed copyright ownership in materials created by Soos, Five Guys began requiring its outside architects to place Five Guys’ CMI into the infringing plans using the Soos works. Soos claimed that Five Guys required its architects to do this in an attempt to mislead other third party architects into believing that Five Guys owned the copyrights in the templates. These allegations were sufficient to plead intent.¹⁷⁸³

With respect to the requirement that false CMI be conveyed in connection with the work, the court found that Soos’ complaint and attached exhibits demonstrated that each page of the architectural templates included a CMI title block stating: “THESE DRAWINGS AND SPECIFICATIONS ARE THE CONFIDENTIAL AND PROPRIETARY PROPERTY OF FIVE GUYS ENTERPRISES, LLC AND SHALL NOT BE COPIED OR REPRODUCED WITHOUT WRITTEN AUTHORIZATION.”¹⁷⁸⁴ This title block appeared directly on each page of the templates at issue. Soos alleged that these templates contained Soos’ copyright work from the architectural plans. The court found that this CMI title block was clearly conveyed in connection with the copyrighted work as it was physically proximate to the copyrighted work, being directly on the page containing the copyrighted material. The court therefore ruled that Soos had stated a claim under Section 1202(a).¹⁷⁸⁵

k. Michael Grecco Prods. v. Time USA

In 2000 and 2005, the plaintiff signed two substantially similar agreements with Time Magazine which granted to Time licenses to use three of the plaintiff’s photos on its covers. Years later, Time began working with a company called Pixels to facilitate the sale of print-on-demand products from Time’s “Cover Store,” which featured decades of Time covers, including the covers at issue in this case. On Pixel’s web site, a shopper could view the covers via a “full resolution preview,” which displayed the covers with a watermark that superimposed the name of the web site, “fineartamerica.com.” Alongside the covers, the artist was listed as “Time.” The

¹⁷⁸¹ Id. at *10.

¹⁷⁸² Id.

¹⁷⁸³ Id. at *11.

¹⁷⁸⁴ Id. at *12.

¹⁷⁸⁵ Id. at *12-13.

plaintiff alleged a claim for falsification of CMI under Section 1202(a) and the defendants filed a motion to dismiss.¹⁷⁸⁶

The court found that the plaintiff's claim improperly conflated the photos with the covers. Here, Time created unique covers using the plaintiff's photos, on which Time overlaid the Time logo, the trademarked Time red border, and text. At no time did the defendants claim ownership of the photos. Instead, the watermark and attribution represented the defendants' reproduction rights with respect to the covers. In the agreements, Time had retained the right to reproduce the covers as derivative works. The court ruled that a party that puts its own CMI on work distinct from work owned by a copyright holder is not liable under Section 1202(a), even if the party's work incorporates the copyright holder's work. Here, the watermark and attribution identified rights with respect to the covers, not the photos, which were just one element of the covers. Accordingly, the court granted the defendants' motion to dismiss.¹⁷⁸⁷

(3) Exceptions and Limitations

Sections 1202(d) provides an exception for law enforcement, intelligence, and information security activities. Section 1202(e) limits the liability of persons for violations in the course of analog transmissions by broadcast stations or cable systems if avoiding the activity that constitutes a violation of the CMI integrity provisions is not technically feasible or would create an undue financial hardship.

(c) Remedies for Violations of Sections 1201 and 1202

Civil Remedies. Section 1203 provides civil remedies for any person injured by a violation of Section 1201 or 1202, including temporary and permanent injunctions (although Section 1203(b)(1) contains a provision prohibiting injunctions that constitute prior restraints on free speech or the press protected under the First Amendment), impounding, actual damages and any additional profits of the violator,¹⁷⁸⁸ statutory damages (in the amount of not less than \$200 or more than \$2,500 for each violation of Section 1201, and not less than \$2,500 or more than \$25,000 for each violation of Section 1202), costs and attorneys' fees, and an order for the remedial modification or the destruction of any device or product involved in the violation. Under Section 1203(c)(4), damages may be trebled by the court for repeated violations within a

¹⁷⁸⁶ Michael Grecco Prods. v. Time USA, LLC, 2021 U.S. Dist. LEXIS 140274 at *2-3 (S.D.N.Y. July 27, 2021).

¹⁷⁸⁷ Id. at *11-13.

¹⁷⁸⁸ Section 1203(c) provides:

- (1) **In general.**—Except as otherwise provided in this title, a person committing a violation of section 1201 or 1202 is liable for either –
 - (A) the actual damages and any additional profits of the violator, as provided in paragraph (2), or
 - (B) statutory damages, as provided in paragraph (3).
- (2) **Actual damages.**—The court shall award to the complaining party the actual damages suffered by the party as a result of the violation, and any profits of the violator that are attributable to the violation and are not taken into account in computing the actual damages, if the complaining party elects such damages at any time before final judgment is entered.

three year period. Conversely, under Section 1203(c)(5), damages may be reduced or remitted entirely if the violator proves that it was not aware and had no reason to believe that its acts constituted a violation.

No Registration Requirement for Statutory Damages and Attorneys' Fees. In Design Ideas, Ltd. v. Meijer, Inc.¹⁷⁸⁹ the court held that a copyright registration is not a prerequisite for the recovery of statutory damages or attorneys' fees under Section 1203. The defendants argued that, because the DMCA is part of Title 17, Section 412 of the copyright statute applies to bar statutory damages and attorneys' fees where the copyright is not registered at the time of the alleged violation. The court rejected this argument, ruling that a plain reading of Section 412 demonstrates that the section applies only to statutory damages and attorneys' fees sought under Sections 504 and 505. Section 412 says nothing about registration prior to the infringement as a prerequisite to receiving statutory damages and attorneys' fees sought under Section 1203.¹⁷⁹⁰

Criminal Penalties. Section 1204 provides for criminal penalties for the willful violation of Sections 1201 or 1202 for purposes of commercial advantage or private financial gain. Penalties include fines up to \$1,000,000 and imprisonment for up to 10 years for repeated offenses.¹⁷⁹¹

(1) Statutory Damages and Disgorgement of Profits for Violations of Section 1201

(i) Sony Computer Entertainment America v. Filippiak

In Sony Computer Entertainment America, Inc. v. Filippiak,¹⁷⁹² the court addressed the standard for computing statutory damages for a violation of the anti-circumvention provisions of the DMCA. The defendant Filippiak sold modification chips for the Sony PlayStation 2 console that circumvented the technological copyright protection measures in PlayStation consoles and allowed users to play unauthorized and illegal copies of PlayStation video games. The court found that Filippiak knew at the time he was selling them that the sale of the mod chips was illegal under the DMCA. Filippiak signed an agreement with SCEA that he would stop selling the mod chips, but nevertheless willfully violated the agreement and continued to sell them. Thereafter, he signed a stipulated consent judgment and injunction that prohibited him from marketing or selling the mod chips and agreed to pay \$50,000 in damages, but still continued to sell the mod

¹⁷⁸⁹ 2018 U.S. Dist. LEXIS 122753 (C.D. Ill. July 23, 2018).

¹⁷⁹⁰ Id. at *26-27.

¹⁷⁹¹ The Digital Future Coalition has criticized Section 1202 as too draconian, in that it would impose civil penalties even in cases where no specific intent to infringe or promote infringement can be shown. "In other words, even someone who alters digital identifiers casually could be liable for a minimum of \$2,500 in damages plus costs and attorney's fees." See position paper of the DFC at www.ari.net/dfc/docs/stwip.htm, p. 3.

¹⁷⁹² 406 F. Supp. 2d 1068 (N.D. Cal. 2005).

chips surreptitiously. When he was caught by SCEA doing so, he admitted that he shouldn't have been doing so and entered into a second consent judgment.¹⁷⁹³

Based on various evidence, the court found that Filiplik had sold a minimum of 7,039 circumvention devices and proceeded to adjudicate the amount of statutory damages that Filiplik should pay. The court first ruled, by analogy to a statutory damages case under the Federal Communications Act, that Section 1203(c)(3)(A) authorizes a separate award of statutory damages for each device sold.¹⁷⁹⁴ Because there were no cases construing what "just" means under Section 1203(c)(3)(A), the court looked to cases construing the term under the general statutory damages provision of Section 504(c) of the copyright statute. Under the Section 504(c) case law, courts consider the following factors in determining the amount of a damages award: the expense saved by the defendant in avoiding a licensing agreement; profits reaped by the defendant in connection with the infringement; revenues lost to the plaintiff; the willfulness of the infringement; and the goal of discouraging wrongful conduct.¹⁷⁹⁵ Applying the factors, and particularly considering the willful nature of Filiplik's violations, the court awarded statutory damages of \$800 per device sold before Filiplik entered into the first agreement with SCEA, and the maximum of \$2500 per device sold or shipped thereafter, for a total award of \$5,631,200.¹⁷⁹⁶

(ii) Sony Computer Entertainment v. Divineo

The facts and rulings of the court in Sony Computer Entertainment America, Inc. v. Divineo¹⁷⁹⁷ are reported in Section II.G.1(m)(19) above. As a remedy for the DMCA violations found by the court, the plaintiff elected statutory damages. The court determined that the defendant had sold a total of 10,012 circumvention devices, and that sales of the devices constituted willful infringement, at least with respect to those sales after the filing of the lawsuit in 2004. Although the defendant had decided to stop selling the HDLoader software in early 2005, the defendant offered no credible explanation for its decision to continue selling its other circumvention devices after that point. Accordingly, the court awarded enhanced damages of \$800 per device for sales after the first quarter of 2005 (an estimated 2,913 devices) and the minimum damages of \$200 per device sold before that time, for a total statutory damages award of \$3,750,200.¹⁷⁹⁸

¹⁷⁹³ Id. at 1070-74.

¹⁷⁹⁴ Id. at 1074.

¹⁷⁹⁵ Id. at 1074-75.

¹⁷⁹⁶ Id. at 1075-76.

¹⁷⁹⁷ 457 F. Supp. 2d 957 (N.D. Cal. 2006).

¹⁷⁹⁸ Id. at 966-67.

(iii) Stockwire Research Group v. Lebed

In this case, the court entered a default judgment against the defendants, who were accused of violating Section 1201 by removing technical protection measures from the plaintiffs' documentary presentation, converting it to a Windows media video and posting it on the web without the plaintiffs' permission, and of violating Section 1202 by removing CMI from the video in the form of the copyright notice, the title of the work, the information identifying one of the plaintiffs as the copyright holder, and the name of the other plaintiff who was credited in the work.¹⁷⁹⁹ The plaintiffs sought statutory damages. Following the McClatchey decision, the court ruled that, for purposes of statutory damages for removal of CMI, "each violation" means each time the product with CMI removed was posted for distribution by the defendant (here, three times), regardless of the number of end recipients.¹⁸⁰⁰ However, for purposes statutory damages for violation of the anti-circumvention prohibitions, "per act of circumvention" means each instance in which an end user gained access to the copyrighted material through unlawful circumvention – here, 11,786 unauthorized viewings, for which the court awarded statutory damages of \$200 per viewing, for a total award of \$2,357,200.¹⁸⁰¹ Thus, CMI statutory damages focus on the acts of the defendant, whereas anti-circumvention statutory damages focus on the acts of the recipients.

(iv) MDY Industries, LLC v. Blizzard Entertainment, Inc.

The facts of this case and the court's various rulings on liability are set forth in Section II.G.1(a)(2)(vii) above. Blizzard requested that it should be entitled to a minimum statutory damages award of \$24 million based upon MDY's sales of at least 120,000 Glider licenses (120,000 x \$200). The district court, however, awarded statutory damages of \$6.5 million, the amount of the damage award in the stipulated judgment between the parties. The court refused to make a reduction of damages on the basis of innocent infringement because MDY had designed its Glider software specifically to bypass the plaintiff's Warden software.¹⁸⁰² On appeal, the Ninth Circuit reversed the district court on all rulings except as to MDY's liability for violation of Section 1201(a)(2) of the DMCA and remanded for trial on Blizzard's claim for tortious interference with contract.¹⁸⁰³

(v) Nexon America v. Kumar

The plaintiff was the owner of a massively multiplayer online game called "MapleStory." The defendants operated a network of servers, websites and related products and services called "UMaple" that enabled users to copy, access, and play MapleStory. To play MapleStory on the

¹⁷⁹⁹ Stockwire Research Group, Inc. v. Lebed, 577 F. Supp. 2d 1262, 1265 (S.D. Fla. 2008).

¹⁸⁰⁰ Id. at 1267.

¹⁸⁰¹ Id. at 1268.

¹⁸⁰² MDY Industries, LLC v. Blizzard Entertainment, Inc., 2009 U.S. Dist. LEXIS 38260 at *4-6 (D. Ariz. Apr. 1, 2009).

¹⁸⁰³ MDY Industries, LLC v. Blizzard Entertainment, Inc., 2011 U.S. App. LEXIS 3428 at *2-3 (9th Cir. Feb. 17, 2011).

defendants' servers, users were required to register for an account with UMaple and obtain a copy of the defendants' modified version of the MapleStory client (called "UMaple Launcher"), which bypassed the plaintiff's technical protection measures restricting access to MapleStory.¹⁸⁰⁴ Upon a default judgment against the defendants, the court considered the statutory damages award that the plaintiff was entitled to for violations of Section 1201 by trafficking in the UMaple Launcher. The court concluded that, because each UMaple member necessarily downloaded a copy of the UMaple Launcher, the number of UMaple members (17,938) was a reasonable approximation of the minimum number of DMCA trafficking violations the defendants had committed. The plaintiff sought the maximum amount of statutory damages, but the court rejected that request, observing from other reported cases that courts tend to award the statutory maximum only where doing so would not create a significant windfall for the plaintiff. Accordingly, the court chose the minimum statutory damages amount of \$200 per violation, and awarded statutory damages in the total amount of $\$200 \times 17,938 = \$3,587,600$.¹⁸⁰⁵

(vi) Point 4 Data Corp. v. Tri-State Surgical Supply

In this case, the plaintiff Point 4 Data Corp. (Point 4), a distributor of a medical supply software system called Genesys, licensed the defendant Tri-State to use Genesys and a computer development platform called UniBasic on which Genesys operated. Because the Genesys/UniBasic system repeatedly crashed, Tri-State began looking for a longer term solution to ensure that the system could operate following a server crash. Point 4 offered to upgrade Tri-State with the latest version of UniBasic and Genesys for \$32,637, but Tri-State declined the offer and hired some consultants to repair the problem. The consultants loaded a copy of the Genesys/UniBasic system onto a spare computer and modified the UniBasic code in a way that bypassed the Genesys/UniBasic security system known as the Passport Licensing Security Software (Passport). Passport functioned to confirm that the computer user was running a proper and authenticated version of UniBasic and extracted information from a dongle concerning the number of authorized users. In the event there were licensing violations, such as an unauthorized number of users, Passport would display an error message and UniBasic would terminate execution. The modifications made by the consultants were such that each time a person logged on to UniBasic or Genesys, a script would run that bypassed Passport and its various checks.¹⁸⁰⁶

A magistrate judge recommended a ruling that the bypassing of the Passport security system violated Section 1201. The plaintiffs sought both disgorgement of the defendants' profits and statutory damages. With respect to disgorgement under Section 1203(c)(2), which allows recovery of "any profits of the violator that are attributable to the violation and are not taken into account in computing the actual damages," the plaintiffs argued that, because Tri-State used the software in its daily business of selling medical supplies and surgical equipment, the

¹⁸⁰⁴ Nexon American Inc. v. Kumar, 2012 U.S. Dist. LEXIS 47294 at *3-4, 15 (C.D. Cal. Apr. 3, 2012).

¹⁸⁰⁵ Id. at *15-20.

¹⁸⁰⁶ Point 4 Data Corp. v. Tri-State Surgical Supply & Equipment, Ltd., 2012 U.S. Dist. LEXIS 113791 at *3-10 (E.D.N.Y. June 13, 2012).

entire amount of profits Tri-State earned in its business should be attributable to the software and, by extension the modifications thereto.¹⁸⁰⁷ The court rejected the plaintiffs' position, noting that were it to adopt the plaintiffs' view of what profits are "attributable" to a DMCA violation, it would ignore the plain language of Section 1203(c)(2) and "impermissibly blur the distinction between damages recoverable under the DMCA (in this case, those related to circumvention) and damages recoverable under the copyright statute (those related to use of the underlying protected works)."¹⁸⁰⁸

Instead, the magistrate judge concluded that a DMCA plaintiff seeking to recover indirect profits under Section 1203(c)(2) must establish that the profits have a legally significant causal relationship to the DMCA violation – in this case, that the profits were attributable to the "cracking" of the Passport security system.¹⁸⁰⁹ "This limitation is especially warranted here, in light of the fact that the statute contains no provision shifting the burden of proof onto the defendant; under *section 1203(c)(2)*, the burden remains squarely on the plaintiff to establish the profits attributable to a DMCA violation."¹⁸¹⁰ The court found that the plaintiffs had failed to show sufficient nexus between the circumvention and the defendants' profits. The court noted that it was undisputed that Tri-State was able to utilize the software and run its business without the crack, and had done so for many years, albeit with some hours of disruption following the occasional server crash. The crack was simply the means by which Tri-State was able to avoid having to rely on its consultant to operate the software following a server crash. Accordingly, in the absence of proof of a link between the circumvention and revenue resulting from sales of Tri-State's medical and surgical equipment, the plaintiffs had not shown that all of Tri-State's profits were attributable to the crack.¹⁸¹¹

The plaintiffs then offered three alternative theories for apportioning the defendants' profits. First, the plaintiffs claimed they were entitled to all profits derived from Tri-State invoices processed with Genesys. Second, they proposed that the court make percentage apportionments of profits based on the court's own evaluation of the qualitative contributions to revenues and profitability of Genesys and UniBasic in relation to the overall business. Third, the plaintiffs proposed subtracting from Tri-State's profits an estimate of what Tri-State's net income would have been had it processed orders by hand for a six month period and then switched to a different automated system. The court rejected these proposals on two grounds. First, each of the alternative theories was tied to profits that were calculated based on the *use* of the software, an approach the court found to be more appropriate to a copyright infringement claim. Second, the theories overlooked the fact that even absent the crack, Tri-State would have had the use of and access to the software. Accordingly, the court recommended granting Tri-State's motion for partial summary judgment as to any profits attributable to the crack, noting

¹⁸⁰⁷ *Id.* at *14-16.

¹⁸⁰⁸ *Id.* at *17.

¹⁸⁰⁹ *Id.* at *26.

¹⁸¹⁰ *Id.*

¹⁸¹¹ *Id.* at *26-29.

that the recommendation did not foreclose the plaintiffs from pursuing statutory damages, or as part of their actual damages, the reasonable licensing fee Tri-State avoided in implementing the crack.¹⁸¹²

The magistrate then turned to the plaintiffs' claim for statutory damages under Section 1203(c)(3)(A) for the circumventions accomplished by the crack. The plaintiffs argued that a separate, distinct act of circumvention took place each time a user logged into the modified system, because the crack functioned by launching a script when a user logged in that bypassed the Passport security system. The plaintiff therefore claimed that it was entitled to statutory damages based on 17,394 logins, carrying statutory damages ranging from a minimum of \$3,478,800 to a maximum of \$43,485,000. The defendants argued that, regardless of how the crack operated, the modification of the software was the only legally cognizable act of circumvention. The court reviewed the applicable precedent, and particularly the Stockwire case discussed above, and concluded that the plaintiffs' suggested approach was the correct one.¹⁸¹³ "Here, after the Crack was implemented, it was Tri-State's employees, not third-party end-users, who then circumvented plaintiffs' software. Under these circumstances, the broad language of the statutory damages provision and the sparse precedent construing that provision support the conclusion that, assuming plaintiffs' version of the facts to be true, each user login gave rise to a separate 'act of circumvention.'"¹⁸¹⁴ Accordingly, the magistrate recommended denial of Tri-State's motion for partial summary judgment limiting statutory damages under the DMCA to a single act of circumvention.¹⁸¹⁵

The district court adopted the magistrate's recommendations in full.¹⁸¹⁶ The district court noted in its opinion that it agreed with the magistrate's conclusion "that profits generated by use of a protected work subsequent to an act of circumvention are generally not disgorgeable under the DMCA. ... [I]t would seem counterintuitive to hold that where the defendant accessed a protected work through an act of circumvention, a DMCA plaintiff may recover all the profits attributable to the defendant's use of that work, without bringing any claim for copyright infringement, even though the acts of use are not DMCA violations."¹⁸¹⁷ The court expressed no opinion whether, on similar facts, disgorgement might be appropriate if the plaintiffs could show that Tri-State used the crack to in fact exceed its prior user limit, and that new capability caused a demonstrable increase in Tri-State's sales and revenue. No such showing had been made here. The court also expressed the belief that, even if the DMCA could be interpreted to allow for disgorgement of profits generated through subsequent use of the protected material, the plaintiffs had not drawn an adequate connection between Tri-State's gross profits and the

¹⁸¹² Id. at *31-34.

¹⁸¹³ Id. at *35-42.

¹⁸¹⁴ Id. at *42-43.

¹⁸¹⁵ Id. at *50.

¹⁸¹⁶ Point 4 Data Corp. v. Tri-State Surgical Supply & Equipment, Ltd., 2012 U.S. Dist. LEXIS 113997 (E.D.N.Y. Aug. 13, 2012).

¹⁸¹⁷ Id. at *4.

Genesys/UniBasic software or the crack – merely showing that the software was an important tool in the internal operations of Tri-State’s business did not establish a sufficient causal connection under the DMCA.¹⁸¹⁸ “Furthermore, the lack of a burden-shifting framework for apportioning profits under the DMCA suggests that a plaintiff has a more exacting duty than a copyright plaintiff to show a causal connection between the DMCA violations and the defendant’s profits.”¹⁸¹⁹

Finally, the district court noted that the plaintiffs had not objected to the magistrate’s rejection of their alternative disgorgement theories, and the district court found no clear error in the magistrate’s conclusions on those points. Similarly, no party had objected to the magistrate’s recommendation regarding statutory damages, and finding no clear error, the court adopted the magistrate’s conclusion that, on the facts accepted by both parties for purposes of the instant motion, each user log-in gave rise to a separate act of circumvention under Section 1203(c)(3). The court agreed with the magistrate’s observation that this conclusion would not foreclose Tri-State from factually contesting how the crack operated or the total number of circumventions that occurred.¹⁸²⁰

In subsequent proceedings, the district court adopted the magistrate’s recommendation to strike as untimely substantial portions of two expert declarations submitted, in part, by the plaintiffs to support the copyrightability of the plaintiffs’ software, which was unregistered. The court further adopted the magistrate’s recommendation that the plaintiffs’ DMCA claim should be dismissed because, after striking the relevant portions of the declarations, the evidence remaining in the record was not sufficient to create an issue of fact with respect to the copyrightability of the software. Absent a showing that the software protected by the technological measures that were circumvented was a copyrighted work, the district court granted summary judgment in favor of Tri-State dismissing the plaintiffs’ DMCA claims.¹⁸²¹ On appeal, the Second Circuit affirmed these rulings in a summary order, finding no abuse of discretion with respect to the district court’s rulings.¹⁸²²

(2) Statutory Damages and Disgorgement of Profits for Violations of Section 1202

(i) McClatchey v. The Associated Press

The facts of this case are set forth in Section II.G.1(b)(1)(ii) above. The Associated Press (AP) brought a motion in limine seeking to limit the number of statutory damage awards that the

¹⁸¹⁸ Id. at *7-8, 12.

¹⁸¹⁹ Id. at *9.

¹⁸²⁰ Id. at *14-15.

¹⁸²¹ Point 4 Data Corp. v. Tri-State Surgical Supply & Equip., Ltd., 2013 U.S. Dist. LEXIS 142121 at * 6-22 (E.D.N.Y. Sept. 30, 2013).

¹⁸²² Dynamic Concepts, Inc. v. Tri-State Surgical Supply & Equip., Ltd., 2017 U.S. App. LEXIS 22348 at *3-15 (2d Cir. Nov. 8, 2017) (unpublished).

plaintiff could recover for the distributions of her photograph with CMI removed. The plaintiff claimed entitlement to a separate statutory award for each downstream distribution of the photograph to each of AP's 1,147 subscribers who had received the photograph. AP argued that the distribution of false CMI to all AP subscribers should be treated as only a single violation of the DMCA, entitling the plaintiff to but a single award of statutory damages.¹⁸²³ The court agreed with AP based on Congress' intent in providing statutory damages as an alternative type of damage award:

Presumably, plaintiffs will elect statutory damages only when that calculation exceeds their actual damages. In other words, Congress has determined that in order to deter violations of the DMCA, plaintiffs electing statutory damages may receive a windfall. The Court's definition of the term "violation" will determine the extent of that windfall. This Court concludes that Congress would not have intended to make the statutory damages windfall totally independent of the defendant's conduct. Where one act by Defendant results in mass infringement, it is more likely that actual damages will yield the more favorable recovery. The DMCA damages provisions are clearly focused on the defendant's conduct. *Compare section 1203(c)(3)(A)* (calculating statutory damages "per act"). In essence, the term "each violation" is best understood to mean "each violative act performed by Defendant." Thus, AP would violate the DMCA each time it wrongfully distributed a photograph to its subscribers. In this case, the Court concludes that AP committed only one alleged violative act by distributing the End of Serenity photograph to its PhotoStream subscribers, even though there were 1,147 recipients.¹⁸²⁴

Upon a motion for reconsideration of this ruling, the district court adhered to its original analysis, but certified the issue for interlocutory appeal and stayed all further proceedings pending resolution of that appeal.¹⁸²⁵

(ii) **Goldman v. Healthcare Management Systems**

In this case, the plaintiff sought statutory damages for the defendants' distribution of infringing copies of a computer program with the plaintiff's CMI removed. The court cited the

¹⁸²³ McClatchey v. The Associated Press, 2007 U.S. Dist. LEXIS 40416 at *13 (W.D. Pa. June 4, 2007).

¹⁸²⁴ Id. at *17-18. The plaintiff also sought statutory damages under Section 504 of the copyright statute. Citing Professor Nimmer's treatise, she argued that she was entitled to recover multiple statutory damages awards if a party is found to be jointly and severally liable with multiple parties who are not jointly and severally liable with each other. Id. at *8. The court rejected this argument, based on the language in Section 504(c)(1) that an award of statutory damages may be recovered for all infringements involved in the action "for which *any* two or more infringers are liable jointly and severally" (emphasis added). Id. at *9-10. Based on the presence of the word "any" rather than "all" in the statute, the court concluded that "the most plausible interpretation of the statute authorizes a single award when there is any joint and several liability, even if there is not complete joint and several liability amongst all potential infringers." Id. at *10. Moreover, the court noted that it need not reject Professor Nimmer's position in all circumstances, because in the instant case the only defendant, AP, was jointly and severally liable with all downstream infringers, so the plaintiff was entitled to only a single statutory damages award. Id. at *12.

¹⁸²⁵ McClatchey v. The Associated Press, 2007 U.S. Dist. LEXIS 41969 (W.D. Pa. June 8, 2007).

McClatchey case for the proposition that, for purposes of Section 1203(c)(3) statutory damages, the phrase “for each violation” means each violative act performed by the defendant. However, in the instant case, unlike a television signal or an AP wire story sent simultaneously to all subscribers, the alleged “violation” was not a singular, isolated event, but rather the provision of the same computer program at different times, under different circumstances, to multiple hospitals. Accordingly, there could be a separate statutory damages award for each computer program distributed to a hospital. However, the court further ruled that whether the subsequent distribution to the hospitals of any particular update to those computer programs would constitute an additional separate “violation” of the plaintiff’s copyright was a factual question that would have to be resolved by a jury.¹⁸²⁶

(iii) Stockwire Research Group v. Lebed

See the discussion of this case in Section II.G.1(c)(1)(iii) above.

(iv) Stockart.com v. Engle

The plaintiff Stockart was in the business of licensing downloads of high end digital imagery through the Internet. Although the images were generally created by others, Stockart took title to the copyrights in the works and paid per-download fees to the creators. The defendant performed unauthorized downloads of several of Stockart’s images and used them to create logos, which the defendant posted and sold on his own website. All images on Stockart.com contained a copyright notice and a © symbol at the bottom of the website screen on which each image appeared. On a motion for a default judgment, a magistrate judge found that such notice and symbol constituted protectable CMI, that by incorporating Stockart’s images into his logos, the defendant had removed Stockart’s CMI from the images, that such removal had been intentional, and that the defendant knew that the removal was a violation of the Copyright Act because, in order to establish an account with Stockart, the defendant had been required to acknowledge and accept a copyright warning in order to search and download images on the site, which warning stated that removal of images from the site or their separation from the copyright management information on the site was not authorized and constituted a violation of copyright law.¹⁸²⁷

Accordingly, the magistrate recommended that the district court conclude that Stockart had stated a viable claim for removal of CMI. Citing the Stockwire case, the magistrate noted that each time a defendant unlawfully posts an unauthorized work for distribution on the Internet, a single violation of the CMI provisions occurs for which a statutory damage award may be made. Here, the magistrate found that the defendant had extracted Stockart images into his logos and posted them on websites for sale a total of 34 times, resulting in 34 violations. The

¹⁸²⁶ Goldman v. Healthcare Management Sys., 559 F. Supp. 2d 853, 867-68 (W.D. Mich. 2008).

¹⁸²⁷ Stockart.com, LLC v. Engle, 2011 U.S. Dist. LEXIS 20470 at *3-6, *28-29 (D. Colo. Feb. 18, 2011).

magistrate recommended that the district court award statutory damages of \$10,000 per violation, for a total award of \$340,000.¹⁸²⁸

(v) Granger v. One Call Lender Services

In this case, the plaintiff was the owner of a computer program that estimated the rate or cost of real estate title insurance sold by title insurance agents. The defendants placed an infringing version of the rate calculator program on their website, though later took it down upon receipt of a demand letter from the plaintiff. The plaintiff had placed external copyright notices (“Copyright 1997-2002 by John Granger” and “All Rights Reserved”) and the name of One Call Lender Services, LLC as web developer and author on the computer program, and had embedded within the computer program similar copyright tag lines and a watermark that, if not removed carefully, could leave a tell-tale sign as to the origin of the work. In posting the program onto their site, the defendants had removed these notices and the watermark. The court ruled that such removal violated the DMCA’s CMI provisions on a motion for default judgment.¹⁸²⁹

The plaintiff sought to recover a statutory damages award for the removal of each of the notices. The court rejected this request, ruling that the individual items of CMI that the defendants removed were immaterial. Citing Stockwire, the court noted that the number of violations of the CMI provisions was to be measured by the number of times the unauthorized product was posted on the Internet for distribution. Because the defendants had posted six different versions of the infringing rate calculator program onto the Internet (versions for six different states), the plaintiff was entitled to six awards of statutory damages. Because the plaintiff had sought only the minimum statutory damages award of \$2,500 per violation, the court awarded statutory damages totaling \$15,000.¹⁸³⁰

(vi) Pacific Stock v. MacArthur & Co.

In this case, the defendant posted the plaintiff’s photographic work on its website with the plaintiff’s CMI on the work removed and false CMI inserted in its place. Upon a default judgment, the magistrate judge found that the plaintiff’s actual damages from the defendant’s

¹⁸²⁸ Id. at *39-41. The magistrate also recommended a finding of willful infringement and an award of statutory damages under Section 504(b) for copyright infringement in the amount of \$30,000 per infringed work. The magistrate based this recommendation on testimony that Stockart normally asked small businesses for a license fee of \$10,000 for use of an image in a logo, and the majority of courts awarding statutory damages for willful infringement utilize a benchmark of two to three times the license fee for computing the award. Id. at *38.

¹⁸²⁹ Granger v. One Call Lender Services, LLC, 2012 U.S. Dist. LEXIS 104885 at *2-4, *13 (E.D. Pa. July 26, 2012).

¹⁸³⁰ Id. at *13-14. The court also awarded statutory damages of \$12,000 for copyright infringement. The court rejected the plaintiff’s claim that it should be entitled to a statutory damages award for each infringing derivative work the defendants had created – i.e., versions of the program for New Jersey, Maryland, Florida, Indiana, and Virginia. “Plaintiff is entitled to recover for only one work since Defendants only infringed upon Plaintiff’s single Rate Calculator, and all remaining calculators were merely derivative works of the Rate Calculator.” Id. at *8-10.

act of copyright infringement were the license fee the plaintiff would have charged for the use of the work in the amount of \$7,505. Noting that a statutory damages award under Section 1202 for the CMI violation should bear some relationship to actual damages, the magistrate judge recommended a statutory damages award of \$10,000 under Section 1202 for the CMI violation, and a statutory damages award of \$35,000 under Section 504(c)(1) for willful copyright infringement.¹⁸³¹ The district court adopted the magistrate's recommendations and supporting opinion in full.¹⁸³²

(vii) **Agence France Presse v. Morel**

The facts of this case are set forth in Section II.G.1(b)(1)(ii).e above. Upon cross motions for summary judgment, the court had to resolve a dispute among the parties concerning how statutory damages should be calculated for CMI violations. Specifically, the plaintiff Morel contended that Section 1203(c)(3)(B) allowed him to recover a separate award of statutory damages for each entity that downloaded or received his photos from AFP or Getty with false CMI, which would have generated a statutory damages award to him of between \$4,445,000 (at the minimum statutory amount) and almost \$44,500,000 (at the maximum statutory amount).¹⁸³³

The court rejected this argument based on a comparison of the damages available under Section 1203(c)(3)(B) for violations of Section 1202 with those available under Section 1203(c)(3)(A) for violations of Section 1201. Specifically, the statutory damages available for violations of Section 1201 are an award "per act of circumvention," where the statutory damages available for violations of Section 1202 are "for each violation of § 1202" (not "per act"). The court concluded that the omission of the reference to damages "per act" in Section 1203(c)(3)(B) meant the damages available under that section should not be multiplied based on the number of recipients of the photos at issue in the case. Rather, damages should be assessed per violation – i.e., based on AFP and Getty's actions in uploading or distributing the photos, regardless of the number of recipients of those images. The court noted that its analysis paralleled that in McClatchey, which the court found persuasive, and that other courts had uniformly followed the approach of McClatchey.¹⁸³⁴

In a subsequent opinion, discussed in Section III.C.6(b)(1)(iii).v below, the court determined that both AFP and Getty were direct infringers for the distribution of unauthorized copies of Morel's photos and allowed the case to go to a jury on the copyright infringement claims and the CMI claims. In Nov. 2013, a New York federal jury found that both AFP and Getty

¹⁸³¹ Pacific Stock, Inc. v. MacArthur & Co., 2012 U.S. Dist. LEXIS 128258 at *413-16 (D. Haw. Sept. 10, 2012).

¹⁸³² Pacific Stock, Inc. v. MacArthur & Co., 2012 U.S. Dist. LEXIS 142449 (D. Haw. Oct. 2, 2012).

¹⁸³³ Agence France Presse v. Morel, 934 F. Supp. 2d 547, 583 & n.22 (S.D.N.Y. 2013).

¹⁸³⁴ Id. at 583, citing for support the following cases: Granger v. One Call Lender Servs., 2012 U.S. Dist. LEXIS 104885 at *12-15 (E.D. Pa. July 26, 2012); Stockart.com, LLC v. Engle, 2012 U.S. Dist. LEXIS 20470 at *40-41 (D. Colo. Feb. 18, 2011); Stockwire Research Group, Inc. v. Lebed, 577 F. Supp. 2d 1262, 1266-67 (S.D. Fla. 2008); and Goldman v. Healthcare Mgmt. Sys., 559 F. Supp. 2d 853, 867-68 (W.D. Mich. 2008).

had willfully infringed Morel's copyright in the eight photographs, awarded Morel \$275,000 in actual damages, \$28,889.77 total in infringer's profits, and \$1.2 million in statutory damages; found that AFP and Getty had jointly committed sixteen violations of the CMI provisions of the DMCA for the distribution of false bylines; and awarded Morel an additional \$20,000 for those DMCA violations. Morel elected to receive statutory damages in lieu of actual damages and infringer's profits, and the court entered judgment in the total amount of \$1,220,000. The defendants' subsequent motions for JMOL, new trial and/or remittitur were denied, except Getty's motion for JMOL with respect to Section 1202(b) liability was granted. AFP and Getty remained jointly liable for \$1.2 million in statutory damages, and AFP was held individually liable for \$10,000 of statutory damages under the CMI provisions of the DMCA (one half of the total the jury awarded against AFP and Getty).¹⁸³⁵

(viii) Reilly v. Plot Commerce

The plaintiff, Jennifer Reilly, a photographer, brought claims for copyright infringement and claims under Section 1202(b) for removal of CMI after the defendant Plot Commerce created unauthorized copies of a photo that Reilly took of musician Tim Reynolds, stripped her watermark and copyright notice, and displayed and distributed without permission the altered copies on at least five distinct URLs on its website. On Mar. 11, 2016, the district court granted Reilly's motion for a default judgment against Plot Commerce and referred the action to a magistrate judge to make a recommendation concerning damages, attorneys' fees and costs.¹⁸³⁶

Because Reilly sought statutory damages under both the Copyright Act and the DMCA, the magistrate turned first to the question of whether a plaintiff can recover statutory damages under both the Copyright Act and the DMCA in the same case. Although noting some district court decisions to the contrary within the Second Circuit, the magistrate discussed two recent district court cases in the Circuit that had allowed damage awards under both statutes where appropriate. The magistrate found this to be an appropriate case for an award of damages under both statutes because Plot Commerce had both unlawfully reproduced Reilly's photo and altered the embedded copyright information in it. Moreover, Reilly had been injured in two different ways. Plot Commerce' use of her copyrighted photo without her permission deprived her of the ability to control when and where it would be displayed, as well as the licensing fee she would ordinarily charge for such display. And the removal of her copyright notice and other CMI deprived her of professional recognition for the display on the website.¹⁸³⁷

With respect to statutory damages for copyright infringement, the magistrate found that the act of removing Reilly's CMI from the photo before displaying it demonstrated that Plot Commerce knew its conduct was infringing. The magistrate noted that, where infringement is willful but not truly egregious, courts in the Circuit frequently award statutory damages of between three and five times the cost of the licensing fees the defendant would have paid. Had

¹⁸³⁵ Agence France Presse v. Morel, 2014 U.S. Dist. LEXIS 112436 at *6-7, *10-29 (S.D.N.Y. Aug. 13, 2014).

¹⁸³⁶ Reilly v. Plot Commerce, 2016 U.S. Dist. LEXIS 152154 at *1-2, *17 (S.D.N.Y. Oct. 31, 2016).

¹⁸³⁷ Id. at *19-21.

Reilly licensed the photo to Plot Commerce, she would have charged \$3,052. Accordingly, the magistrate found that an award of \$15,000 in statutory damages under the Copyright Act would be appropriate.¹⁸³⁸

With respect to statutory damages under the DMCA, Section 1203(3)(B) allows an award of statutory damages in the range of \$2,500 to \$25,000 for each violation of Section 1202. However, the magistrate noted that courts had exhibited uncertainty as to what constitutes a single violation of the DMCA and the appellate courts had not yet spoken on the issue. In particular, although some courts had permitted separate awards for the removal of CMI and for the distribution of the altered copyrighted work, there was uncertainty as to whether a plaintiff can recover an award for each copy of a work distributed with altered CMI. The magistrate noted, and agreed with, decisions holding that each act of removal of CMI and each act of addition of false CMI can be a separate violation of the DMCA, although here there was no act of addition.¹⁸³⁹

Reilly argued that she was entitled to five statutory awards for the upload of the photo to Plot Commerce's website because it appeared on five different pages within that website. The magistrate rejected this argument, ruling that where, as here, a violator posts a single image to a single website, it has committed only a single violative act. The court noted that an image or other content need be uploaded only once to a database before it can be used to create multiple dynamic web pages based on the choices made by the user of the site. Reilly had not presented any evidence concerning the architecture of its website and therefore had not established that Plot Commerce uploaded the photo more than once to its website. The magistrate therefore invoked what it found to be the now well-accepted rule of the *McClatchey* case, discussed in Section II.G.1(b)(1)(ii).a above, under which a violator who posts an altered image to a news feed, thereby delivering it directly to multiple recipients, is nonetheless deemed to have committed only a single violation of the DMCA. The magistrate therefore recommended that Reilly be given one award of statutory damages for the removal of CMI in the amount of \$5,000 and another award in the amount of \$5,000 for the posting of the altered photo on Plot Commerce's website, for a total of \$10,000 in statutory damages under the DMCA. The magistrate also recommended an award of \$5,280 in attorneys' fees.¹⁸⁴⁰

The district court, having received no objection to the magistrate's recommendations, adopted them without modification.¹⁸⁴¹

¹⁸³⁸ *Id.* at *24-26.

¹⁸³⁹ *Id.* at *26-30.

¹⁸⁴⁰ *Id.* at *31-34, 38.

¹⁸⁴¹ *Reilly v. Plot Commerce*, 2016 U.S. District LEXIS 160884 at *2 (S.D.N.Y. Nov. 21, 2016).

(3) Whether There is a Right to Jury Trial on Statutory Damages Under Section 1202

(i) Oppenheimer v. Johnson

In Oppenheimer v. Johnson,¹⁸⁴² the plaintiff obtained a default judgment of direct copyright infringement and violation of Sections 1202(b)(1) and 1202(b)(3) for unauthorized posting of his copyrighted photograph on the defendant's website with the CMI removed. The plaintiff elected to take statutory damages under Section 1202 and sought a jury trial on the amount of damages. The court ruled that a plaintiff has no statutory right to a jury trial on the issue of statutory damages under Section 1202 of the DMCA, and no constitutional right to a jury trial after a default judgment.¹⁸⁴³

With respect to a statutory right, the court noted the Supreme Court's ruling in Feltner v. Columbia Pictures Televisions, Inc.¹⁸⁴⁴ that the language of Section 504(c) of the copyright statute does not grant a right to have a jury assess statutory damages. The court then ruled that, likewise, the DMCA has no provision that grants a right to a jury trial on the issue of damages and the plaintiff therefore had no statutory right to a jury trial as to statutory damages under the DMCA.¹⁸⁴⁵ Nor did the plaintiff have a constitutional right to a jury trial in these circumstances. The court cited authority holding that Fed. R. Civ. Pro. 55 presupposes that a default judgment extinguishes the constitutional right to a jury trial, and noted that the overwhelming weight of authority to consider the issue holds that the Seventh Amendment does not guarantee a jury trial after default, including several cases denying jury trial requests in copyright cases following a default. The court therefore ruled that the plaintiff had no constitutional right to a jury trial on his statutory claim for damages under the DMCA because a default had been entered in the case.¹⁸⁴⁶

(ii) Huffman v. Activision Publ'g

In Huffman v. Activision Publ'g, Inc.,¹⁸⁴⁷ the court reached the opposite conclusion from the Oppenheimer v. Johnson court. The court first found that the language of Section 1203(b) was too broad for it to conclusively determine on semantic grounds whether there was a statutory grant of a jury trial. Although Section 1203(b) permits "the court" to "award damages under subsection (c)," at no place does Section 1203 articulate whether a judge or jury should decide statutory damages. The court therefore read Section 1203 within the context of other similar provisions in the copyright statute, and found that it could not distinguish any meaningful

¹⁸⁴² 2020 U.S. Dist. LEXIS 130502 (W.D.N.C. July 23, 2020).

¹⁸⁴³ Id. at *9-16.

¹⁸⁴⁴ 523 U.S. 340, 346 (1998).

¹⁸⁴⁵ Oppenheimer, 2020 U.S. Dist. LEXIS at *11-12.

¹⁸⁴⁶ Id. at *13-14.

¹⁸⁴⁷ 2021 U.S. Dist. LEXIS 106838 (E.D. Tex. June 8, 2021).

differences between the statutory damages authorized in Section 504(c) and Section 1203(c)(3)(B). Though the language between the two statutes was somewhat different, there were significant parallels that compelled the court to conclude that Congress intended for courts to continue viewing statutory copyright remedies as legal remedies. The court therefore concluded that Congress intended for the Section 1203(c)(3)(B) remedy to mirror the Section 504(c) common law remedy, thus giving a right to a jury trial under Section 1203(c)(3)(B).¹⁸⁴⁸

(4) Whether Copyright Registration is a Prerequisite to a DMCA Claim or Remedies

(i) Design Ideas v. Meijer

In Design Ideas, Ltd. v. Meijer, Inc.¹⁸⁴⁹ the court held that a copyright registration is not a prerequisite for the recovery of statutory damages or attorneys' fees under Section 1203. The defendants argued that, because the DMCA is part of Title 17, Section 412 of the copyright statute applies to bar statutory damages and attorneys' fees where the copyright is not registered at the time of the alleged violation. The court rejected this argument, ruling that a plain reading of Section 412 demonstrates that the section applies only to statutory damages and attorneys' fees sought under Sections 504 and 505. Section 412 says nothing about registration prior to the infringement as a prerequisite to receiving statutory damages and attorneys' fees sought under Section 1203.¹⁸⁵⁰

(ii) Diamondback Indus. v. Repeat Precision

The plaintiff asserted a claim for violation of Section 1202(b). The defendant sought dismissal of the claim on the ground that the plaintiff had not registered the copyright for the work from which CMI had allegedly been removed or altered. The court denied the motion to dismiss, ruling that copyright registration is not a prerequisite to an action under Section 1202 for several reasons. First, because an action under Section 1202 is not an action for infringement, the registration requirement of Section 411(a) is inapplicable. Although Section 1202(b) does mention "infringement," such infringement is not the subject of the civil action. Instead, the reference to infringement is used to describe the scienter requirement, wherein the defendant must know that the removal or alteration of CMI will induce, enable, facilitate, or conceal an infringement of a copyright. Although a DMCA claim requires the defendant to know of potential infringement, such requirement does not necessitate registration because infringement can occur absent registration.¹⁸⁵¹

¹⁸⁴⁸ Id. at *16-19.

¹⁸⁴⁹ 2018 U.S. Dist. LEXIS 122753 (C.D. Ill. July 23, 2018).

¹⁸⁵⁰ Id. at *26-27. Accord Recif Res., LLC v. Juniper Capital Advisors, L.P., 2020 U.S. Dist. LEXIS 175431 at * 28-29 (S.D. Tex. Sept. 24, 2020) (citing Meijer).

¹⁸⁵¹ Diamondback Indus. v. Repeat Precision, LLC, 2019 U.S. Dist. LEXIS 193637 at *2, 3-5 (N.D. Tex. Nov. 7, 2019).

Second, the court noted that Section 411(a) need not apply to the DMCA merely because other provisions of Title 17 do. Section 411(a)'s terms expressly limit its application to civil actions for infringement of a copyright.¹⁸⁵² Third, the Supreme Court's decision in Fourth Estate Public Benefit Corp. v. Wall-Street.com, LLC,¹⁸⁵³ relied on by the defendant, pertained to what constitutes adequate registration under Section 411(a) before bringing a lawsuit to enforce ownership rights in a copyright. A DMCA action is not a suit to enforce such ownership rights.¹⁸⁵⁴

Finally, the court found that the one case cited by the defendant in which a court found that the DMCA requires registration was not persuasive because it did not provide any analysis in arriving at that conclusion.¹⁸⁵⁵ In any event, that decision was not binding precedent on the court, and the court noted that several other district courts had reached the opposite conclusion.¹⁸⁵⁶ Accordingly, the court denied the defendant's motion to dismiss.¹⁸⁵⁷

(5) Whether Mitigation is a Defense to Statutory Damages Under the DMCA

(i) Energy Intelligence Grp. v. Kayne Anderson Capital Advisors

In this case, the plaintiff published a daily newsletter called *Oil Daily* that provided news and analysis about the North American petroleum industry. The defendant purchased a single subscription to *Oil Daily*, but one of its employees shared access to that subscription with several fellow employees and other third parties – initially by sharing his username and password and later by distributing PDF copies of the publication – in violation of the subscription agreement. The plaintiff brought claims for numerous instances of copyright infringement and violation of the CMI provisions of the DMCA. At trial, the jury found 425 alterations of CMI and imposed statutory damages of \$2500 per alteration, but also concluded that the defendant could reasonably have avoided almost all the copyright and DMCA violations but failed to do so because, despite having knowledge of the violations, the defendant sat on its hands by conducting no investigation and by failing to warn the employee of the Copyright Act's hefty statutory damages provision. Based on the jury's failure to mitigate, the district court awarded the plaintiff nothing on its DMCA claims. On appeal, the parties agreed that the plaintiff's failure to mitigate is a relevant factor in deciding what statutory damages ought to be imposed, but

¹⁸⁵² Id. at *6.

¹⁸⁵³ 139 S. Ct. 881 (2019).

¹⁸⁵⁴ Diamondback, 2019 U.S. Dist. LEXIS 193637 at *6-7.

¹⁸⁵⁵ Id. at *7 (referring to Sims v. Viacom, Inc. 2012 U.S. Dist. LEXIS 11485 (W.D. Pa. Jan. 31, 2012)).

¹⁸⁵⁶ Diamondback, 2019 U.S. Dist. LEXIS 193637 at *7 (citing Gattoni v. Tibi, LLC, 254 F. Supp. 3d 659, 663-64 (S.D.N.Y. 2017); Exec. Corp. v. Oisoan, LLC, 2017 U.S. Dist. LEXIS 159922 at *4 (M.D. Tenn. Sept. 28, 2017); ECIMOS, LLC v. Carrier Corp., 2016 U.S. Dist. LEXIS 59191 at *9 (W.D. Tenn. May 4, 2016); Playboy Enters. Int'l Inc. v. Mediatakeout.com LLC, 2016 U.S. Dist. LEXIS 29249 at *5 (S.D.N.Y. Mar. 8, 2016); Med. Broad. Co. v. Flaiz, 2003 U.S. Dist. LEXIS 22184 at *3 (E.D. Pa. Nov. 25, 2003)).

¹⁸⁵⁷ Diamondback, 2019 U.S. Dist. LEXIS 193637 at *8.

disagreed over whether failure to mitigate can act as an absolute defense to preclude liability altogether.¹⁸⁵⁸

The Fifth Circuit, noting that this was an issue of first impression, held that failure to mitigate is not a complete defense to copyright or DMCA claims for statutory damages, although it can be taken into account in setting the amount of statutory damages. The court began by reviewing the duty to mitigate under common law, noting that it refers to methods of apportioning damages in view of a plaintiff's reasonable efforts to reduce loss *after* an injury occurs, not before. The relevant authorities establish that mitigation rules apply to consequential damages. Actual damages and defendant's profits under the Copyright Act are a form of consequential damages. By contrast, the court concluded that statutory damages are designed in part to discourage wrongful conduct and may be imposed to sanction and vindicate the statutory policy against copyright infringement. The court's conclusion was based on the fact that the 1976 Copyright Act revised the 1909 Act by establishing an unequivocal right on the part of copyright owners to opt for statutory damages at any time before final judgment, reinforced by the fact that several modern appellate decisions have emphasized the deterrence purposes of statutory damages, which allow for enhancement in case of willful infringement.¹⁸⁵⁹

In view of this, the court concluded that statutory damages under the Copyright Act are not solely intended to approximate actual damages, but rather also serve a deterrence purpose. Statutory damages under the Copyright Act are thus distinct from the type of damages that are typically calculated according to rules of mitigation, and failure to mitigate should therefore not constitute an absolute defense to statutory damages under Section 504.¹⁸⁶⁰

The court noted that statutory damages under Section 1203 have notable parallels and some divergences to statutory damages under Section 504. Under both provisions, the plaintiff may seek either actual damages and the defendant's profits, or statutory damages. At any time before final judgment, the plaintiff may elect to recover statutory damages. Unlike Section 504, however, the trial court, in its discretion, may reduce or remit the *total award* if the defendant proves the violations were innocent. While noteworthy, the court concluded that the differences do not suggest that mitigation should be available as an absolute defense in DMCA claims. Like statutory damages under Section 504(c), the structure of statutory damages under Section 1203 indicates an intent to deter, not just compensate. The court may treble damages, including statutory damages, if the defendant is a repeat offender. And textually, nothing in Section 1203 requires statutory damages to be lined to actual damages. Accordingly, the court held that mitigation is not an absolute defense to DMCA claims either.¹⁸⁶¹

¹⁸⁵⁸ Energy Intelligence Grp., Inc. v. Kayne Anderson Capital Advisors, L.P., 948 F.3d 261, 264-66, 275-76 (5th Cir. 2020).

¹⁸⁵⁹ Id. at 273-74.

¹⁸⁶⁰ Id. at 274.

¹⁸⁶¹ Id. at 276.

With respect to the DMCA violations, the parties had agreed that if mitigation is not a complete defense, the court should enter judgment for the plaintiff. The court therefore entered judgment in favor of the plaintiff in the amount of \$2,500 (the amount the jury elected to impose) for each of the defendant's 425 violations of the CMI provisions of the DMCA, or \$1,062,500.¹⁸⁶²

(6) Statute of Limitations

In Hirsch v. Rehs Galleries, Inc.,¹⁸⁶³ the court held that the Copyright Act's three year statute of limitations applies to actions under Section 1202, including the discovery rule, under which claims do not accrue until actual or constructive discovery of the relevant infringement.¹⁸⁶⁴

(7) Jurisdictional Issues – Blueport Co. v. United States

In Blueport Co. v. United States,¹⁸⁶⁵ the Court of Claims ruled that the United States cannot be sued under the DMCA's anti-circumvention provisions because the DMCA contains no clear waiver of sovereign immunity, and waiver under the DMCA could not be inferred from waiver under the copyright laws because the DMCA is not a copyright statute. The Federal Circuit affirmed this ruling on appeal for the same reasons invoked by the Court of Claims, and also noted the rule that the Court of Claims lacks jurisdiction to adjudicate claims created by statutes, like the DMCA, which specifically authorized jurisdiction in the district courts.¹⁸⁶⁶

(8) Arbitrability of Claims Under the DMCA

In Boss Worldwide LLC v. Crabill,¹⁸⁶⁷ the court held that DMCA claims are arbitrable. The plaintiff and the defendants entered into an Operating Agreement to govern a new business they jointly formed to teach customers how to sell products online. After the parties had a falling out and went their separate ways, the defendant filed a takedown notice with YouTube, claiming that one of the plaintiff's promotional videos contained copyrighted content the plaintiff was not authorized to use and asking that YouTube take it down. The plaintiff alleged the takedown notice contained misrepresentations and inaccurate information in violation of Section 512(f). The plaintiff submitted a counter-notification to YouTube but as of the date of the lawsuit, the video had not been restored. In the course of an earlier mediation to attempt to resolve issues

¹⁸⁶² Id. at 280-81. The court's rulings with respect to the basis for the CMI violations are discussed in Section II.G.1(b)(1)(iv).h above. On remand, the district court ordered a new trial on statutory damages with respect to the copyright claims. Energy Intelligence Grp. V. Kayne Anderson Capital Advisors, LP, 2020 U.S. Dist. LEXIS 236220 (S.D. Tex. Dec. 16, 2020).

¹⁸⁶³ 2020 U.S. Dist. LEXIS 32926 (S.D.N.Y. Feb. 26, 2020).

¹⁸⁶⁴ Id. at *7-9.

¹⁸⁶⁵ 80 U.S.P.Q.2d 1585 (Ct. Fed. Claims 2006).

¹⁸⁶⁶ Blueport Co. v. United States, 533 F.3d 1374, 1382-84 (Fed. Cir. 2008).

¹⁸⁶⁷ 2020 U.S. Dist. LEXIS 47462 (S.D.N.Y. Mar. 16, 2020).

stemming from the breakdown of their business relationship, including contractual disputes and other claims, the plaintiff provided the DMCA complaint to the mediator and demanded the withdrawal of the takedown notice as one of its requirements for settlement. Because the Operating Agreement contained an arbitration clause applicable to “any dispute over the provisions of this operating agreement and in other disputes among the members,” the defendant argued that the DMCA claim must be arbitrated. The court agreed that the DMCA claim fell within the scope of the arbitration clause.¹⁸⁶⁸ It found no indication Congress had precluded DMCA claims from arbitration¹⁸⁶⁹ and therefore ruled that the claim was arbitrable by the terms of the Operating Agreement and ordered the parties to arbitrate the dispute.¹⁸⁷⁰

(d) Alternative Approaches to the DMCA That Did Not Pass

Two of the alternatives bills that were introduced to implement the WIPO treaties which did not pass, S. 1146 and H.R. 3048, would have prohibited only certain defined circumvention conduct, rather than devices. Specifically, Section 1201 of S. 1146 and H.R. 3048 provided that no person, “for the purpose of facilitating or engaging in an act of infringement, shall engage in conduct so as knowingly to remove, deactivate or otherwise circumvent the application or operation of any effective technological measure used by a copyright owner to preclude or limit reproduction of a work or a portion thereof.” Thus, these bills would not have banned circumvention undertaken for reasons other than facilitating or engaging in infringement, such as fair uses. In addition, Section 1201 of these bills expressly defined “conduct” not to include manufacturing, importing or distributing a device or a computer program.

Although Section 1201(a) of these bills referred only to technological measures used to preclude or limit reproduction of a copyrighted work, and did not refer to access to a copyrighted work (as is included in the DMCA), the definition of “effective technological measure” in Section 1201(c) of these bills included two references to access. Specifically, “effective technological measure” was defined as information included with or an attribute applied to a transmission or a copy of a work in a digital format which “encrypts or scrambles the work or a portion thereof in the absence of access information supplied by the copyright owner; or includes attributes regarding access to or recording of the work that cannot be removed without degrading the work or a portion thereof.” This was a much more specific and narrower definition of effective technological measure than that contained in the DMCA.

Unlike Section 1201, Section 1202 of S. 1146 and H.R. 3048 was largely identical to Section 1202 of the DMCA with respect to removal, alteration or falsification of CMI. The most important difference was that Section 1202 of S. 1146 and H.R. 3048 contained language making clear that the conduct governed by that Section did not include the manufacturing, importing or

¹⁸⁶⁸ Id. at *1-5, *8-9.

¹⁸⁶⁹ Id. at *9 (citing Packeteer, Inc. v. Valencia Sys., Inc., 2007 U.S. Dist. LEXIS 21348 at *3 (N.D. Cal. Mar. 6, 2007) (rejecting argument that “Congress conferred exclusive jurisdiction over copyright and DMCA claims on the federal courts”)).

¹⁸⁷⁰ Boss Worldwide, 2020 U.S. Dist. LEXIS 47462 at *10-11.

distributing of a device (curiously, there was no reference to a computer program, as there was in the exclusion from Section 1201 of those bills).

(e) The Battle Between Content Owners and Technology Companies Over Built-In Technological Measures

An ongoing battle has been developing between holders of copyright on content, most notably the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA), and technology companies over whether manufacturers of devices that can be used to play, copy or distribute copyrighted content should be required to build in to such devices technological protection measures that restrict access to or the use of such copyrighted content. In effect, content owners have sought through various proposed federal legislation to mandate the inclusion of technological measures in devices that would be covered by the anti-circumvention provisions of the DMCA. Computer, consumer electronic, and other technology companies have resisted such legislation mightily, arguing that they must be free to design their own products without legislative strictures.

On Jan. 14, 2003, the RIAA, the Business Software Alliance (BSA),¹⁸⁷¹ and the Computer Systems Policy Project (CSPP)¹⁸⁷² announced that they had reached agreement on a core set of seven principles to guide their public policy activities in the 108th Congress (2003) regarding the distribution of digital content.¹⁸⁷³ Pursuant to the agreement, the recording companies agreed that they would not seek government intervention to mandate technical solutions to prevent digital piracy and would in most instances oppose legislation that would require computers and consumer electronics devices to be designed to restrict unauthorized copying of audio and video material. In turn, the BSA and CSPP would not support legislation that seeks to clarify and bolster the rights of persons to use copyrighted material in digital format. Notably absent from the agreement were consumer electronics companies, who felt that legislation was needed to ensure that consumers can make fair use of digital copyrighted material even when secured with technology to prevent illegal copying, and the MPAA, whose members continued to be concerned that digital television broadcasts and movies copied from DVDs would soon be traded over the Internet in high volumes.¹⁸⁷⁴

¹⁸⁷¹ Members of the BSA include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, Cisco Systems, CNC/Mastercam, Dell, Entrust, HP, IBM, Intel, Internet Security Systems, Intuit, Macromedia, Microsoft, Network Associates, Novell, PeopleSoft, SeeBeyond, Sybase, and Symantec. "Recording, Technology Industries Reach Groundbreaking Agreement on Approach to Digital Content Issues," available on the BSA web site as of Jan. 15, 2003 at www.bsa.org/usa/press/newsreleases//2003-01-14.1418.phtml.

¹⁸⁷² Members of the CSPP include Dell, Intel, HP, Motorola, NCR, IBM, EMC, and Unisys. *Id.*

¹⁸⁷³ The seven policy principles may be found on the BSA web site at www.bsa.org/usa/policyres/7_principles.pdf.

¹⁸⁷⁴ Amy Harmon, "Music Industry Won't Seek Government Aid on Piracy" (Jan. 15, 2003), available as of Jan. 15, 2003 at www.nytimes.com/2003/01/15/business/15PIRA.html.

2. Anticircumvention Provisions Under the European Copyright Directive

The European Copyright Directive adopts the approach of the DMCA, in that it would outlaw both conduct and the manufacture or distribution of devices that could be used to defeat technological copyright protections. With respect to conduct, Article 6(1) provides that member states “shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.”¹⁸⁷⁵ The language of Article 6(1) includes a knowledge requirement that is not expressly present in the prohibition of Section 1201(a)(1)(A) of the DMCA. But unlike the DMCA, there are no enumerated exceptions to the ban on circumvention in the European Copyright Directive.¹⁸⁷⁶

Like the DMCA, the European Copyright Directive does not require that the circumvention of the technical measures be done for the purpose of facilitating or engaging in an act of infringement. However, the commentary to Article 6 elaborates on the requirement of knowledge by the party liable for the circumvention in a way that suggests a standard of liability that may be somewhat akin to that of the *Sony* case in the United States: “This [requirement of knowledge] would allow for the necessary flexibility – a fundamental element for the industry – not to cover activities which are related to devices which may serve a legal or illegal use and are carried out without the actual knowledge that they will enable circumvention of technological protection devices.”¹⁸⁷⁷ It is therefore important how broadly this provision will be implemented by individual member states.

With respect to the manufacture or distribution of devices that could be used to defeat technological copyright protections, Article 6(2) provides that member states “shall provide adequate legal protection against the manufacture, import, distribution, sale, rental,

¹⁸⁷⁵ Notwithstanding the general prohibition on circumvention of effective technological measures, Article 6(4) provides that, “in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.”

¹⁸⁷⁶ Schollenberger, *supra* note 309, at 12. The European Copyright Directive attempts to deal with this issue via Article 6(4), which states that “Member States should promote voluntary measures taken by right holders, including the conclusion and implementation of agreements between rights holders and other parties concerned, to accommodate achieving the objectives of certain exceptions or limitations provided for in national law.” It further states that in the absence of such voluntary measures or agreements, within a reasonable period of time Member States are obliged to take appropriate measures to ensure that right holders provide beneficiaries of such exceptions or limitations with “appropriate means” of benefiting from them, by modifying an implemented technological protection measure or by other means. What such “appropriate measures” would be remains unclear. *Id.*

¹⁸⁷⁷ Commentary to Art. 6, ¶ 2.

advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

- (a) are promoted, advertised or marketed for the purpose of circumvention of, or
- (b) have only a limited commercially significant purpose or use other than to circumvent, or
- (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.”

The foregoing three criteria are very similar to the criteria enumerated in the prohibition of technology, devices and services contained in Sections 1201(a)(2) and 1201(b) of the DMCA. However, by prohibiting preparatory activities to circumvention, Article 6(2) goes further than the WIPO Copyright Treaty requires.¹⁸⁷⁸

One possible difference between the European Copyright Directive and the DMCA may lie in the scope of what types of technological measures are prohibited from circumvention. Specifically, the prohibitions of the DMCA are expressly directed toward technology, devices and services that circumvent technological measures that effectively *control access* to a copyrighted work and *protect rights of a copyright holder*. By contrast, the definition of “technological measures” in the European Copyright Directive, at first glance, seems directed only toward protecting rights of a copyright holder, and not restricting access. Article 6(3) defines the expression “technological measures” to mean “any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorized by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC.”

However, the concept of access control seems to come into the European Copyright Directive indirectly, through the definition of “effective.” Specifically, Article 6(3) provides that technological measures shall be deemed “effective” where “the use of a protected work or other subject-matter is controlled by the rightholders through application of an *access control* or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective” (emphasis added). Thus, through the interaction of these definitions of “technological measures” and “effective,” it appears that the European Copyright Directive effectively prohibits the circumvention of technological measures that both control access and that protect the rights of a copyright holder, just as does the DMCA.

An important thing to note is that the anti-circumvention provisions of Article 6 of the European Copyright Directive do not apply to computer programs. Instead, a different, and more limited, set of anti-circumvention provisions apply to computer programs under Directive

¹⁸⁷⁸ Harrington & Berking, *supra* note 308, at 6.

91/250/EEC on the Legal Protection of Computer Programs (the “European Software Directive”), discussed in the next paragraph. Article 2(a) of the European Copyright Directive states that the “Directive shall leave intact and shall in no way affect existing Community provisions relating to the legal protection of computer programs.” And Recital 50 of the European Copyright Directive states that its harmonized legal protection “does not affect the specific provisions on protection provided for by Directive 91/250/EEC [the European Software Directive]. In particular, it should not apply to the protection of technological measures used in connection with computer programs, which is exclusively addressed in that Directive.”

The narrower anti-circumvention provisions applicable to computer programs are set forth in Article 7(1)(c) of the European Software Directive, which requires member states to provide appropriate remedies against “any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program.” There are a couple of important distinctions between the anti-circumvention provisions of the European Software Directive and those of the European Copyright Directive:

- The anti-circumvention provisions of the European Software Directive are aimed at preventing the manufacture and distribution of circumvention devices. Unlike the relevant provisions of the European Copyright Directive, they do not prohibit the actual conduct of circumvention itself.

- The anti-circumvention provisions of the European Software Directive apply only to devices that have circumvention as their sole intended purpose, which is narrower than the anti-circumvention provisions of the European Copyright Directive that apply to devices that have circumvention as their primary purpose, or are promoted, advertised or marketed for the purpose of circumvention, or have only a limited commercially significant purpose or use other than to circumvent.

Article 7(1) of the European Copyright Directive deals with CMI, which the European Copyright Directive denominates “electronic rights management information.” Specifically, Article 7(1) requires member states to prohibit any person knowingly performing without authority any of the following acts:

- “(a) the removal or alteration of any electronic rights-management information;

- (b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive or under Chapter III of Directive 96/9/EC from which electronic right-management information has been removed or altered without authority,

if such person knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of any copyright or any rights related

to copyright as provided by law, or of the *sui generis* right provided in Chapter III of Directive 96/9/EC.”

Article 7(2) defines “rights management information” broadly to mean “any information provided by rightholders which identifies the work or other subject-matter referred to in this Directive or covered by the *sui generis* right provided for in Chapter III of Directive 96/9/EC, the author or any other rightholder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information. The first subparagraph shall apply when any of these items of information is associated with a copy of, or appears in connection with the communication to the public of, a work or other subject matter referred to in this Directive or covered by the *sui generis* right provided for in Chapter III of Directive 96/9/EC.”

The scope of Article 7 is potentially narrower than that of the United States implementing legislation. The prohibitions of Article 7(1) are all expressly directed to “electronic” rights-management information. In addition, the commentary states that Article 7 “aims only at the protection of electronic rights management information, and does not cover all kinds of information that could be attached to the protected material.”¹⁸⁷⁹ By contrast, the definition of CMI under the DMCA is broad enough to cover more than just electronic information.

3. Anti-Circumvention Provisions in Other Foreign Countries

Some countries outside the European Union have adopted anti-circumvention provisions in their copyright laws. For example, effective March 2001 Australia added a new Section 116A to its copyright law, which prohibits circumvention of a “technological protection measure,” defined as “a device or product, or a component incorporated into a process, that is designed, in the ordinary course of its operation, to prevent or inhibit the infringement of copyright in a work or other subject-matter.”¹⁸⁸⁰ In October of 2005, the High Court of Australia unanimously ruled that distributing mod chips to overcome region coding on the PlayStation video games was not a violation of Section 116A. The court reasoned that the region coding scheme did not constitute a technological protection measure.¹⁸⁸¹

In July of 2003, the Federal Court of Australia held that region access codes in CD-ROMs of PlayStation games, as well as a companion chip in the PlayStation console, constituted a valid “technological protection measure,” and that the defendant had violated Section 116A by distributing modification chips that overcame the regional restrictions on play of the games.¹⁸⁸²

¹⁸⁷⁹ Commentary to Art. 7, ¶ 1.

¹⁸⁸⁰ “Australian Federal Court Upholds Region Coding Restrictions on Video Game System,” *BNA’s Electronic Commerce & Law Report* (Aug. 20, 2003) at 802.

¹⁸⁸¹ Murray Griffin, “Fair Use Ruling on TPMs Raises Concern That Australian Law May Conflict with FTA,” *BNA’s Electronic Commerce & Law Report* (Oct. 12, 2005) at 982.

¹⁸⁸² *Id.*

In March of 2005, a German court, on the basis of the anti-circumvention provision of German copyright law, prohibited the German news site Heise from linking in an online article to a site where circumvention software was made available.¹⁸⁸³

4. Fair Use

(a) United States Legislation That Did Not Pass

Both S. 1146 and H.R. 3048 – neither of which were ultimately adopted by Congress – contained identical provisions with respect to application of the fair use doctrine in a digital environment. These bills would have amended Section 107 of the copyright statute (the fair use exemption) in two ways. First, they would have added an amendment providing that the fair use doctrine applies to uses of a copyrighted work “by analog or digital transmission.” Second, they would have added a new sentence to Section 107 providing that, in making a determination concerning fair use, a court should give no independent weight to the means by which the work has been performed, displayed or distributed under the authority of the copyright owner, or the application of an effective technological measure to protect the work. The import of this provision appears to have been (i) to clarify that digital uses of a copyrighted work may be a fair use notwithstanding that the copyright owner has authorized use of the work only in other media or modes and (ii) that the fair use exemption may apply even if an effective technological measure must be circumvented to use the work (as in the case of reverse engineering). However, as discussed above, both the RealNetworks and the Reimerdes cases held that fair use is not a defense to a claim for violation of the anti-circumvention provisions of Section 1201(a); thus, the fact that a defendant circumvented a technological protection measure in order to gain access to a copyrighted work to make fair uses of it does not provide a defense.

(b) The European Copyright Directive

Article 5(3) of the European Copyright Directive permits member states to adopt limitations to the rights of reproduction and of communication or making available to the public for the following fair use purposes:

- for illustration for teaching or scientific research for noncommercial purposes, as long as the source, including the author’s name, is indicated;
- for the benefit of people with a disability, which are directly related to the disability and of a noncommercial nature, to the extent required by the specific disability;
- use of short excerpts in connection with the reporting of current events, so long as the source, including the author’s name, is indicated;

¹⁸⁸³ “Court Prohibits Linking to Circumvention Software” (Mar. 7, 2005), available as of Mar. 8, 2005 at <http://constitutionalcode.blogspot.com/2005/03/court-prohibits-linking-to.html>.

- quotations for purposes such as criticism or review of a work that has been lawfully made available to the public, so long as the source, including the author’s name, is indicated and the use is in accordance with fair practice;
- for public security or proper performance of an administrative or judicial procedure;
- use of political speeches or public lectures to the extent justified by the informatory purpose and provided that the source, including the author’s name, is indicated;
- use during public religious or official celebrations;
- use of works of architecture or sculpture made to be located permanently in public places;
- incidental inclusion of a work in other material;
- use for advertising the public exhibition or sale of artistic works to the extent necessary to promote the event;
- use for caricature, parody or pastiche;
- use in connection with the demonstration or repair of equipment;
- use of an artistic work in the form of a building or a drawing or plan of a building for reconstructing the same;
- use by communication or making available to individual members of the public by dedicated terminals in publicly accessible libraries, educational establishments, museums or archives for noncommercial purposes; and
- use in certain other cases of minor importance where exceptions or limitations already exist under national law, provided that concern only analog uses and do not affect the free circulation of goods and services within the EC.

Article 5(5) provides that in all cases, the limitations “shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder.”

5. Expansion of Library/Archives Exemptions

Section 404 of the DMCA expands the scope of the exemption in Section 108 of the copyright statute for libraries and archives. Specifically, Section 108 authorizes libraries and archives to make three copies of works for preservation purposes, rather than one. Section 108 also deletes the requirement that the copies be made “in facsimile form.” According to Rep. Boucher, this phrase in the pre-amended version of Section 108 had been read to preclude the

use of digital technologies to preserve works.¹⁸⁸⁴ Under the amended Section 108, a work may be copied for preservation purposes if it is currently in the collections of the library or archives and, if reproduced in digital format, it is not otherwise distributed in that format and is not made available to the public in that format outside the premises of the library or archives.

6. Distance Education

Section 403 of the DMCA requires that, within six months after enactment, the Register of Copyrights submit to Congress recommendations on how to promote distance education through digital technologies, including interactive digital networks, while maintaining an appropriate balance between the rights of copyright owners and the needs of users of copyrighted works. The DMCA lists a number of factors that should be considered in making such recommendations.¹⁸⁸⁵

7. Copying in the Course of Computer Maintenance or Repair

Title III of the DMCA added a new subsection to Section 117 of the copyright statute, providing that it is not an infringement for an owner or lessee of a machine to make or authorize the making of a copy of a computer program if such copy is made solely by virtue of the activation of a machine that lawfully contains an authorized copy of the program, for purposes only of maintenance or repair of that machine, provided the copy is used in no other manner and is destroyed immediately after the maintenance or repair is completed, and, with respect to any computer program or portion thereof that is not necessary for that machine to be activated, such is not accessed or used other than to make the new copy by virtue of the activation of the machine.

¹⁸⁸⁴ "Latest Copyright Treaty Implementation Bill Limits Scope of Shrink-Wrap Agreements," *BNA's Electronic Information Policy & Law Report* (Nov. 26, 1997) at 1232.

¹⁸⁸⁵ The factors include: The need for an exemption from exclusive rights of copyright owners for distance education through digital networks; the categories of works to be included under the exemption; the extent of appropriate quantitative limitations on the portions of works that may be used under the exemption; the parties who should be entitled to the benefits of the exemption; the parties who should be designated as eligible recipients of distance education materials under the exemption; whether and what types of technological measures can or should be employed as a safeguard against unauthorized access to and use or retention of copyrighted materials as a condition of eligibility for any exemption; and the extent to which the availability of licenses for the use of copyrighted works in distance education through interactive digital networks should be considered in assessing eligibility for the exemption.

Both S. 1146 and H.R. 3048 would have afforded a broader expansion of the exemptions in Section 110(2) of the copyright statute for certain performances or displays of copyrighted works for instructional activities performed by government or nonprofit educational institutions. The bills would have extended this exemption to distributions of a work, in addition to performances and displays, to cover the distribution of a work over a computer network. The bills would also have expanded the exemption from nondramatic literary or musical works to all works, and extended the exemption to apply to students officially enrolled in the course, not only courses held in a classroom.

This amendment to the copyright statute was deemed necessary by its sponsors in view of judicial decisions such as MAI Systems Corp. v. Peak Computer,¹⁸⁸⁶ discussed above, and Triad Sys. v. Southeastern Express Co.,¹⁸⁸⁷ which held that copying portions of a computer program to memory in the course of turning on and running the machine constitutes a “reproduction” under Section 106 of the copyright statute. Under these decisions, a service technician who is not the owner or licensee of the system software commits copyright infringement by even booting up the machine for maintenance or repair. The revisions to Section 117 made by the DMCA change this result. In Telecomm Technical Services Inc. v. Siemens Rolm Communications,¹⁸⁸⁸ the court ruled that this provision is to be applied retroactively.

The scope of the computer maintenance and repair right was construed very broadly in the case of Storage Technology Corporation v. Custom Hardware Engineering & Consulting, discussed in Section II.G.1(a)(14)(iv) above.

8. Other Provisions of the DMCA

The DMCA contains the following other miscellaneous provisions:

(a) Evaluation of Impact of Copyright Law on Electronic Commerce

Section 104 of the DMCA requires the Register of Copyrights and the Assistant Secretary for Communications and Information of the Commerce Department to study and report to Congress within two years of enactment of the DMCA with respect to the DMCA’s impact on “the development of electronic commerce and associated technology,” and “the relationship between existing and emergent technology” and Sections 109 and 117 of the copyright statute. The report required under Section 104 was issued in August of 2001 and is available online at www.loc.gov/copyright/reports/studies/dmca/dmca_study.html.

In a nutshell, the executive summary of the report concludes, “We are not persuaded that title I of the DMCA has had a significant effect on the operation of sections 109 and 117 of title 17. The adverse effects that section 1201, for example, is alleged to have had on these sections cannot accurately be ascribed to section 1201. The causal relationship between the problems identified and section 1201 are currently either minimal or easily attributable to other factors such as the increasing use of license terms. Accordingly, none of our legislative recommendations are based on the effects of section 1201 on the operation of sections 109 and 117.”¹⁸⁸⁹

¹⁸⁸⁶ 991 F.2d 511 (9th Cir. 1993), cert. dismissed, 114 S. Ct. 672 (1994).

¹⁸⁸⁷ 64 F.3d 1330 (9th Cir. 1995), cert. denied, 116 S. Ct. 1015 (1996).

¹⁸⁸⁸ No. 1:95-CV-649-WBH (N.D. Ga. July 6, 1999).

¹⁸⁸⁹ The quoted language is from the opening paragraph of Section III of the Executive Summary of the report. The Executive Summary may be found at www.loc.gov/copyright/reports/studies/dmca/dmca_executive.html.

The report does, however, recommend two legislative changes: (i) that the copyright statute be amended “to preclude any liability arising from the assertion of a copyright owner’s reproduction right with respect to temporary buffer copies that are incidental to a licensed digital transmission of a public performance of a sound recording and any underlying musical work”¹⁸⁹⁰ and (ii) that Congress “either (1) amend section 109 to ensure that fair use copies are not subject to the first sale doctrine or (2) create a new archival exemption that provides expressly that backup copies may not be distributed.”¹⁸⁹¹ The recommendation with respect to temporary buffer copies is discussed further in Section III.E.4(b) below.

(b) Clarification of the Authority of the Copyright Office

Section 401 of the DMCA clarifies the authority of the Copyright Office. Specifically, it provides that, in addition to the functions and duties of the Register of Copyrights already enumerated in the copyright statute, the Register shall perform the following functions: (1) Advise Congress on national and international issues relating to copyright; (2) Provide information and assistance to federal departments and agencies and the judiciary on national and international issues relating to copyright; (3) Participate in meetings of international intergovernmental organizations and meetings with foreign government officials relating to copyright; and (4) Conduct studies and programs regarding copyright, including educational programs conducted cooperatively with foreign intellectual property offices and international intergovernmental governments.¹⁸⁹²

¹⁸⁹⁰ Id. section III.b.2.c.

¹⁸⁹¹ Id. section III.b.3.b.

¹⁸⁹² This provision is the outcome of a skirmish that developed between Bruce Lehman, the former Commissioner of Patents & Trademarks and Mary Beth Peters, the Register of Copyrights. Commissioner Lehman was pushing for creation of a new position of Under Secretary of Commerce for Intellectual Property Policy, or what some referred to as an “intellectual property czar.” Under a proposed provision that did not pass Congress, the duties of the new position would have been to: (1) Promote exports of goods and services of the United States industries that rely on intellectual property; (2) Advise the President, through the Secretary of Commerce, on national and certain international issues relating to intellectual property policy, including issues in the areas of patents, trademarks, and copyrights; (3) Advise Federal departments and agencies on matters of intellectual property protection in other countries; (4) Provide guidance, as appropriate, with respect to proposals by agencies to assist foreign governments and international intergovernmental organizations on matters of intellectual property protection; (5) Conduct programs and studies related to the effectiveness of intellectual property protection throughout the world; (6) Advise the Secretary of Commerce on programs and studies relating to intellectual property policy that are conducted, or authorized to be conducted, cooperatively with foreign patent and trademark offices and international intergovernmental organizations; and (7) In coordination with the Department of State, conduct programs and studies cooperatively with foreign intellectual property offices and international intergovernmental organizations.

The effect of this provision would have been to vest responsibility for public policy issues relating to copyright (as well as trademarks and patents) in the new position, relegating the Copyright Office to a largely administrative role primarily related to registration of copyrights. The Copyright Office was obviously opposed to this, and appears to have been the victor of the skirmish, for Section 401 makes clear that responsibility for public policy issues relating to copyright lies with the Copyright Office, led by the Register of Copyrights.

(c) Ephemeral Recordings

Section 402 of the DMCA expands the rights under Section 112 of the copyright statute of broadcast radio or television stations licensed by the FCC to make ephemeral recordings of material transmitted via analog broadcasts to include recordings of a performance of a sound recording in digital format on a non-subscription basis. This expansion of the ephemeral recording right was made necessary by the Digital Performance Right in Sound Recordings Act of 1995, which granted sound recording copyright owners the exclusive right to publicly perform their works by means of digital audio transmissions.

Section 402 responds to Congress' concern, expressed in the Conference Report, that if use of copy protection technologies becomes widespread, a transmitting organization might be prevented from engaging in its traditional activities of assembling transmission programs and making ephemeral recordings permitted by Section 112 of the copyright statute. Accordingly, Section 402 provides that where a transmitting organization entitled to make an ephemeral recording is prevented from making such recording by the application by the copyright owner of a technical measure that prevents reproduction of the work, the copyright owner must make available to the transmitting organization the necessary means for making the recording, if it technologically feasible and economically reasonable to do so. If the copyright owner fails to do so in a timely manner, then the transmitting organization is granted an exemption from liability under the provisions of the DMCA that would otherwise prohibit the transmitting organization from circumventing the technical measure.

(d) Statutory Licenses With Respect to Performances of Sound Recordings

Section 405 of the DMCA contains provisions relating to statutory compulsory licenses with respect to performances of sound recordings, including digital audio transmissions, and sets up procedures for voluntary negotiation proceedings to determine reasonable terms and rates of royalty payments for public performances of sound recordings. According to the Conference Report, Section 405 was intended to achieve two purposes: first, to further a stated objective of Congress when it passed the Digital Performance Right in Sound Recordings Act of 1995 to ensure that recording artists and record companies will be protected as new technologies affect the ways in which their creative works are used; and second, to create fair and efficient licensing mechanisms that address the complex issues facing copyright owners and copyrights users as a result of the rapid growth of digital audio services.¹⁸⁹³ The details of these provisions, which are lengthy and quite complex, are beyond the scope of this paper.

(e) Assumption of Contractual Obligations Related to Transfers of Rights in Motion Pictures

Section 406 of the DMCA adds a new Section 4001 to Title 28 of the United States Code to address the problem caused by the failure of motion picture producers to obtain, as part of a collective bargaining agreement, assumption agreements from distributors to make residual

¹⁸⁹³ *Id.* at 79-80.

payments. New Section 4001 provides generally that transfers of copyright ownership not limited to public performance rights by exhibitors in motion pictures produced subject to a collective bargaining agreement will be subject to the assumption agreements applicable to the copyright ownership being transferred that are required by the applicable collective bargaining agreement, provided that the transferee knows or has reason to know at the time of the transfer of the collective bargaining agreement, or, in the event of a court order confirming an arbitration award against the transferor under the collective bargaining agreement, the transferor does not have the financial ability to satisfy the award within 90 days after the order is issued. Security interests and transfers related to exercise of security interests in such motion pictures are exempted from the provisions of Section 4001.

(f) Protection of Certain Industrial Designs

Title V of the DMCA adds a new Chapter 13 to the copyright statute entitled “Protection of Original Designs.” Although as currently enacted, Chapter 13 protects only vessel hull designs¹⁸⁹⁴ with a copyright-like design right, its provisions are drafted in the form of a general industrial design protection statute. Merely by changing a definition in the statute, Congress can in the future easily extend the scope of industrial designs that are protected. To obtain protection, the statute requires that the owner of the design register the design with the Copyright Office within two years of making the design public as embodied in a useful article. Title V of the DMCA originally provided that the design protection statute would be effective for an initial trial period of two years. However, Section 5005(a)(2) of the Intellectual Property and Communications Omnibus Reform Act of 1999¹⁸⁹⁵ deleted this two-year sunset provision.

(1) Protection of Designs Embodied in Useful Articles

Section 1301(a) of the statute provides generally that the “designer or other owner of an original design of a useful article which makes the article attractive or distinctive in appearance to the purchasing or using public may secure the protection provided by this chapter upon complying with and subject to this chapter.” Section 1301(b)(2) defines a “useful article” as a “vessel hull or deck,”¹⁸⁹⁶ including a plug or mold, which in normal use has an intrinsic utilitarian

¹⁸⁹⁴ Title V overrules Bonita Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141 (1989), in which the Supreme Court barred states from protecting unpatented boat hulls because such protection conflicts with the federal policy favoring free competition in inventions not qualifying for patent protection.

¹⁸⁹⁵ P.L. 106-113 (1999).

¹⁸⁹⁶ Section 1301(b)(3), as amended by Section 5005(a)(2) of the Intellectual Property and Communications Omnibus Reform Act of 1999, P.L. 106-113, defines a “vessel” as “a craft--(A) that is designed and capable of independently steering a course on or through water through its own means of propulsion; and (B) that is designed and capable of carrying and transporting one or more passengers.” Under Section 1301(b)(4), as amended by the Vessel Hull Design Protection Amendments of 2008, P.L. 110-434, a “hull” is “the exterior frame or body of a vessel, exclusive of the deck, superstructure, masts, sails, yards, rigging, hardware, fixtures, and other attachments” and a “deck” is “the horizontal surface of a vessel that covers the hull, including exterior cabin and cockpit surfaces, and exclusive of masts, sails, yards, rigging, hardware, fixtures, and other attachments.”

function that is not merely to portray the appearance of the article or to convey information. An article which normally is part of a useful article shall be deemed to be a useful article.” It is apparent that, although this definition is currently limited to vessel hulls and decks, the phrase “vessel hull or deck” in the definition could easily be replaced with a generic phrase such as “article,” thereby extending protection to general industrial designs. Alternatively, enumerated categories of designs in addition to vessel hulls or decks could easily be added to the definition.

(2) Originality

The statute establishes a low threshold of originality for protection. Specifically, Section 1301(b)(1) provides that a design is original “if it is the result of the designer’s creative endeavor that provides a distinguishable variation over prior work pertaining to similar articles which is more than merely trivial and has not been copied from another source.” Although this is a low threshold, it is interesting to note that it is a higher threshold than under copyright law. Specifically, under copyright law a work of authorship is deemed original if it is simply not copied from another work, whether or not it embodies a distinguishable variation from prior works. Thus, two photographers could take identical photos from the edge of the Grand Canyon by standing in the same places, and each would produce an “original,” and therefore copyrightable, photo. By contrast, under the design statute, a second designer who, as a result of independent development, happens to produce a design the same as a preexisting design, has not created an “original” design.

(3) Exclusions from Protection

Section 1302 excludes protection for a design that is:

- (1) not original;
- (2) staple or commonplace, such as a standard geometric figure, a familiar symbol, an emblem, or a motif, or another shape, pattern, or configuration which has become standard, common, prevalent, or ordinary;
- (3) different from a design excluded by clause (2) only in insignificant details or in elements which are variants commonly used in the relevant trades;
- (4) dictated solely by a utilitarian function of the article that embodies it;¹⁸⁹⁷ or
- (5) embodied in a useful article that was made public by the designer or owner anywhere in the world more than two years¹⁸⁹⁸ before registering the design with the

¹⁸⁹⁷ Section 1301(a)(2), as amended by the Vessel Hull Design Protection Amendments of 2008, P.L. 110-434, provides, “The design of a vessel hull, deck, or combination of a hull and deck, including a plug or mold, is subject to protection under this chapter, notwithstanding section 1302(4).”

¹⁸⁹⁸ Section 1302(5) as originally published at 112 Stat. 2906 reads “1 year” at this point in clause (5). However, this is apparently an error, for Section 1310(a) states that protection shall be lost “if application for registration of the design is not made within 2 years after the date on which the design is first made public” (emphasis added).

Copyright Office.¹⁸⁹⁹ (Under Section 1310(b), a design is “made public” when an existing useful article embodying the design “is anywhere publicly exhibited, publicly distributed, or offered for sale or sold to the public by the owner of the design or with the owner’s consent.”)

(4) Adaptations of Unprotectable Elements

Section 1303 provides that a design employing elements not protectable under Section 1302 may nevertheless be protected if such design is a substantial revision, adaptation, or rearrangement of such unprotectable elements.

(5) Duration of Protection and Design Notice

Protection commences on the earlier of the date of publication of the design’s registration or its first being made public, and lasts for a term of ten years (including through the end of the calendar year of the tenth year). Section 1306 requires designs that have been made public to bear a design notice comprised of the words “Protected Design,” the abbreviation “Prot’d Des.,” or the letter “D” with a circle or the symbol “*D*”; the year of the date on which protection commenced; and the name of the owner or a recognized abbreviation or alternative name. After registration, the registration number may be used in the design notice in lieu of the second and third notice elements enumerated above. Under Section 1307, omission of the notice does not invalidate protection, but prevents any recovery of damages against an infringer until the infringer has notice of the design rights, and no injunction may issue against such infringer unless the owner reimburses the infringer for any reasonable expenditure or contractual obligation incurred before receiving notice.

(6) Rights of a Design Owner and Limitations

Under Section 1308, the owner of a protected design has the exclusive right to make, have made, or import, for sale or for use in trade, any useful article embodying the design, and to sell or distribute for sale or for use in trade any useful article embodying the design. Section 1309 places a number of limitations on who may be deemed infringers, however:

-- First, under Section 1309(b), a seller or distributor who did not make or import an infringing article is itself deemed an infringer only if (i) the seller or distributor induced or acted in collusion with a manufacturer or importer (other than by merely placing an order for the infringing articles) or (ii) failed to make a prompt and full disclosure of its

¹⁸⁹⁹ Under the provisions of Section 1310, the registration of a design requires, among other things, the specific name of the useful article embodying the design, and two copies of a drawing or other pictorial representation of the useful article having one or more views adequate to show the design in a form and style suitable for reproduction. Section 1310(i) provides that when a design is embodied in more than one useful article, the design is protected as to all useful articles when protected as to one of them, but only one registration is required for the design. Section 1313(c) sets up certain procedures by which a registered design may be challenged and canceled. Under Section 1314, a registration constitutes prima facie evidence of the facts stated in the registration certificate.

source of the infringing article upon request of the design owner, and the seller or distributor orders or reorders the infringing articles after receiving notice by registered or certified mail that the design is protected.

-- Second, a person who makes, has made, imports, sells or distributes an article embodying an infringing design which was created without such person's knowledge that the design was protected and was copied from the protected design.

-- Third, a person who incorporates into that person's product of manufacture an infringing article acquired from another in the ordinary course of business or who, without knowledge of the protected design embodied in an infringing article, makes or processes the infringing article for the account of another in the ordinary course of business, is not an infringer, except to the extent such person would be deemed an infringer under the seller/distributor provisions above.

(7) Standard of Infringement

Under Section 1309(a), to establish infringement, a design owner must prove that an "infringing article" has been made, imported, sold or distributed without the design owner's consent. Section 1309(e) defines an "infringing article" as one embodying a design that was "copied" from a protected design, and provides that an infringing article "is not an illustration or picture of a protected design in an advertisement, book, periodical, newspaper, photograph, broadcast, motion picture, or similar medium." The statute does not directly define what it means to "copy" a design. However, Section 1309(e) provides, "A design shall not be deemed to have been copied from a protected design if it is original and not substantially similar in appearance to a protected design."¹⁹⁰⁰ Strictly speaking, this provision enumerates only one way in which an alleged infringer can rebut an allegation of copying, and it does not state that this is the only way. However, it is unclear what happens when an accused design is, by coincidence, substantially similar to a protected design but can be shown to have been independently developed. Such a showing of independent development would be sufficient to avoid liability under copyright law, and it seems logical that it should be sufficient to prove that the design was not "copied" under the design statute as well.

(8) Benefit of Foreign Filing Date

Under Section 1311, an applicant for registration of a design in the United States can claim the benefit of an earlier filing date in a foreign country for registration of the same design if (i) the foreign country extends similar design protection to citizens of the United States, and (ii)

¹⁹⁰⁰ It is unclear what the relationship is between the standard of "substantially similar" for infringement purposes and the standard of "distinguishable variation" (in the definition of "original") for purposes of protectability. However, Section 1309(f) provides that if an accused infringer introduces an earlier work which is identical to an allegedly protected design or so similar as to make a prima facie showing that such design was copied, then the burden shifts to the owner of the allegedly protected design to prove its originality.

the application is filed in the United States within six months after the earliest date on which any such foreign application was filed.

(9) Vesting and Transfer of Ownership

Under Section 1320, design rights vest in the creator of the design, or, in the case of a design made within the regular scope of the designer's employment, in the employer. Property rights in a design may be assigned or mortgaged by an instrument in writing, and any such conveyance is void as against a subsequent purchaser or mortgagee for valuable consideration unless it is recorded in the Copyright Office within three months after its execution or before the date of such subsequent purchase or mortgage.

(10) Remedies of Injunctive Relief, Damages, Attorneys' Fees and Destruction

Section 1322 permits a court to award preliminary and permanent injunctive relief against infringement of protected designs. Under Section 1323(a), the owner of a protected design may recover "damages adequate to compensate for the infringement," but the damages awarded "shall constitute compensation and not a penalty." Section 1323(a) permits the court to increase the damages to such amount, not exceeding \$50,000 or \$1 per copy, whichever is greater, as the court deems just. As an alternative, under Section 1323(b), the court may award the owner of the protected design the infringer's profits resulting from the sale of the infringing copies "if the court finds that the infringer's sales are reasonably related to the use" of the protected design. The owner is required to prove only the amount of the infringer's sales, and the infringer must then prove its expenses against such sales. Section 1323(d) allows the court to award attorneys' fees to the prevailing party and Section 1323(e) allows the court to order the destruction of plates, molds, and the like used to make infringing articles. Section 1323(c) sets up a three year statute of limitations.

(11) Private Rights of Action Against Pirated Designs

Section 1326 affords a powerful remedy for victims of pirated designs. Specifically, that Section allows a private right of action to recover civil fines of not more than \$500 per offense for false marking with a design notice knowing that the design is not protected. The civil fines are split equally between the private plaintiff and the United States.

(12) Relation to Design Patents and Retroactive Effect

Finally, Section 1329 provides that the issuance of a design patent terminates any protection for the original design under the design statute, and Section 1332 provides that the design statute has no retroactive effect.

(g) Limitation of Liability of Online Service Providers

The DMCA contains elaborate provisions and safe harbors that limit the liability of online service providers for copyright infringement occurring through their services. These provisions are discussed in Section III.C.6 below.

(h) Subpoenas to Service Providers

Section 512(h) of the DMCA sets up a procedure through which a copyright owner may obtain a subpoena through a United States district court directing the service provider to release the identity of an alleged direct infringer acting through the service provider's system or network. The subpoena is issued by the clerk of any United States district court upon a request by the copyright owner (or one authorized to act on the owner's behalf) containing the proposed subpoena, "a copy of a notification described in subsection (c)(3)(A)," and a sworn declaration ensuring that the subpoena is solely to obtain the identity of the alleged infringer, which information will be used only to protect rights to the copyright.¹⁹⁰¹ The subpoena, in turn, authorizes and orders the recipient service provider "to expeditiously disclose" information sufficient to identify the alleged infringer.¹⁹⁰² The clerk "shall expeditiously issue" the subpoena if it is in proper form, the declaration is properly executed, and "the notification filed satisfies the provisions of subsection (c)(3)(A)."¹⁹⁰³ The service provider, upon receipt of the subpoena, "shall expeditiously disclose" the information required by the subpoena to the copyright owner (or authorized person).¹⁹⁰⁴ The issuance, delivery and enforcement of subpoenas is to be governed (to the extent practicable) by the provisions of the Federal Rules of Civil Procedure dealing with subpoenas duces tecum.¹⁹⁰⁵

(1) Jurisdictional Issues

The issue of where subpoenas under Section 512(h) must be sought and where they can be served was tested in two lawsuits brought by Massachusetts universities against the RIAA, Massachusetts Institute of Technology v. RIAA¹⁹⁰⁶ and Boston College v. RIAA.¹⁹⁰⁷ In those cases, the universities challenged the service in Massachusetts of Section 512(h) subpoenas issued by a federal district court in Washington, D.C. The court ruled that Fed. R. Civ. P. 45(a)(2) and (b)(2), which require a subpoena to issue from the district in which the production is to be made, do

¹⁹⁰¹ 17 U.S.C. § 512(h)(2).

¹⁹⁰² *Id.* § 512(h)(3).

¹⁹⁰³ *Id.* § 512(h)(4).

¹⁹⁰⁴ *Id.* § 512(h)(5).

¹⁹⁰⁵ *Id.* § 512(h)(6).

¹⁹⁰⁶ 1:03-MC-10209-JLT (D. Mass. Aug. 7, 2003).

¹⁹⁰⁷ 1:03-MC-10210-JLT (D. Mass. Aug. 7, 2003).

not permit a Section 512(h) subpoena for production issued in Washington, D.C. to be validly served in Massachusetts.¹⁹⁰⁸

The RIAA contended that service of the subpoenas was proper because of language within the DMCA that the RIAA contended trumps Fed. R. Civ. P. 45. Specifically, the RIAA pointed to Section 512(h)(1), which authorizes a copyright owner to request the clerk of “any” U.S. district court to issue a subpoena. Second, Section 512(h)(5) requires the service provider to disclose the requested information “notwithstanding any other provision of law.” Third, while Section 512(h)(6) provides that the rules regarding service of subpoenas will govern to the “greatest extent practicable,” that provision also contains an important carve out: “unless otherwise provided by this section.” The court rejected the RIAA’s arguments, ruling that Section 512(h) does not trump the ordinary rules regarding service of subpoenas under the Federal Rules of Civil Procedure.¹⁹⁰⁹

(2) RIAA v. Verizon Internet Services

The scope of Section 512(h) was first tested in the case of In re Verizon Internet Services, Inc.¹⁹¹⁰ In that case, the Recording Industry Association of America (RIAA) served a subpoena under Section 512(h) on Verizon Internet Services seeking identifying information about an anonymous copyright infringer allegedly using Verizon’s network to download copyrighted songs through peer-to-peer software provided by Kazaa. Along with the subpoena, RIAA provided Verizon with a list of more than 600 files allegedly downloaded by the user on one day. The subpoena included the user’s IP address and the time and date when the songs were downloaded, and a declaration, under penalty of perjury, that the information was sought in good faith and would only be used in connection with protecting the rights of RIAA members.¹⁹¹¹

Verizon refused to comply with the subpoena, arguing that, because Section 512(h) requires a notice under Section 512(c)(3)(A) to accompany the subpoena application, the subpoena power applies only if the infringing material is stored or controlled on the Service Provider’s system or network under subsection (c). Verizon further argued that, because it provided the alleged infringer only with an Internet connection, it fell under subsection (a) of Section 512 and was thus outside the subpoena authority of Section 512(h).¹⁹¹² The RIAA sought to enforce the subpoena against Verizon in court.

The district court rejected Verizon’s arguments and ruled that the subpoena power of Section 512(h) applies to all service providers within the scope of the DMCA, not just to those service providers storing information on a system or network at the direction of a user. The

¹⁹⁰⁸ “District of Columbia Court Lacks Authority to Issue DMCA Subpoenas to Boston Schools,” *BNA’s Patent, Trademark & Copyright Journal* (Aug. 15, 2003) at 458.

¹⁹⁰⁹ Id.

¹⁹¹⁰ 240 F. Supp. 2d 24 (D.D.C. 2003).

¹⁹¹¹ Id. at 28.

¹⁹¹² Id. at 29.

court held that the plain language of Section 512(h) compelled this result, because it employs the term “service provider” repeatedly, and Section 512(k) provides two definitions of the term “service provider” – one directed to service providers falling under Section 512(a) and another directed to service providers falling under Sections 512(b) – (d).¹⁹¹³ The court rejected Verizon’s contention that it should infer that the subpoena authority applies only to subsection (c) in view of the reference in subsection (h)(2)(A) to the notification requirement of subsection (c)(3)(A). The court noted that “the notification provision in subsection (c) is also referenced elsewhere in the DMCA, including in subsections (b)(2)(E) and (d)(3). The latter references confirm the expectation that notifications like that described in subsection (c)(3) will at times be needed in settings under subsections (b) and (d), and hence are not confined to subsection (c) settings.”¹⁹¹⁴ The court also rejected a number of constitutional challenges to the Section 512(h) subpoena power identified by *amici curiae*, noting that Verizon itself had not directly asserted that the subpoena power in Section 512(h) was unconstitutional and that the issues raised by the *amici curiae* had not been fully briefed by the RIAA.¹⁹¹⁵ In a subsequent ruling, the district court issued a more elaborated opinion on a number of constitutional challenges to the subpoena power in Section 512(h) raised by Verizon and *amici curiae* and again rejected those challenges.¹⁹¹⁶

On appeal, the D.C. Circuit reversed.¹⁹¹⁷ The appellate court held, based on both the terms of Section 512(h) and its overall structure that a subpoena may be issued only to an ISP engaged in storing on its servers, or linking to, material that is infringing or the subject of infringing activity, and not to an ISP acting only as a conduit for data transferred between two

¹⁹¹³ *Id.* at 31.

¹⁹¹⁴ *Id.* at 32-33. Verizon also relied on the fact that under subsection (c)(3)(A)(iii) a copyright owner must identify the infringing material “that is to be removed or access to which is to be disabled.” Verizon argued that in order to remove or disable access to the material, the material must be stored on its system, thereby indicating that Congress intended Section 512(h) to apply only to those service providers who store infringing material on their systems. The court rejected this argument. “[A] subpoena issued pursuant to subsection (h) is used to identify the infringer, not to force the service provider to remove material or disable access to it. The requirement for the notification is simply that it identify the infringing material to be removed, not that removal be effectuated. In addition, a copyright owner can meet the requirement under subsection (c)(3)(A)(iii) if it can disable access to material. Here, Verizon certainly can disable access to the material by terminating the account altogether.” *Id.* at 33 n.5. Since Verizon was a Section 512(a) service provider, and the requirement in subsection (c) to remove or disable access to infringing material stored on the service provider’s system is not applicable to subsection (a), it is unclear what the court’s reference to Verizon’s ability to disable access to material by terminating accounts was intended to mean. Perhaps that service providers who are subject to the Section 512(a) safe harbor must nevertheless terminate the accounts of repeat infringers in order to qualify for the safe harbor, per the provisions of Section 512(i). This is only a possible implication, however, and the point of the court’s passage is that Section 512(h) is focused on identification of the infringer, not removal or disabling of access to infringing material.

¹⁹¹⁵ *Id.* at 41-44.

¹⁹¹⁶ *In re Verizon Internet Services, Inc.*, 257 F. Supp. 2d 244, 257-68 (D.D.C. 2003). The court also rejected Verizon’s argument that Section 512(h) violates Art. III of the Constitution because it authorizes federal courts to issue binding process in the absence of a pending case or controversy. *Id.* at 248-57.

¹⁹¹⁷ *Recording Industry Ass’n of Am. v. Verizon Internet Services, Inc.*, 351 F.3d 1229 (D.C. Cir. 2003), *cert. denied*, 543 U.S. 924 (2004).

Internet users. With respect to the language of Section 512(h) itself, the court noted that Section 512(h)(4) makes satisfaction of the notification requirement of Section 512(c)(3)(A) a condition precedent to issuance of a subpoena, which notification requirement must identify and provide information sufficient to locate infringing material that is to be removed or access to which is to be disabled. The court held that an ISP that is not storing the allegedly infringing material on its servers cannot “remove” or “disable access to” the infringing material no matter what information the copyright owner may provide.¹⁹¹⁸

The RIAA contended that an ISP can “disable access” to infringing material, even when it is providing only conduit functions, by terminating the offending subscriber’s Internet account. The court rejected this argument, noting that the DMCA, in Sections 512(j)(1)(A)(i) and 512(j)(1)(A)(ii), sets up distinct statutory remedies in the form of injunctions against providing access to infringing material and injunctions against providing access to a subscriber who is engaged in infringing activity.¹⁹¹⁹ “These distinct statutory remedies establish that terminating a subscriber’s account is not the same as removing or disabling access by others to the infringing material resident on the subscriber’s computer.”¹⁹²⁰ The court further noted that the RIAA’s notification had identified absolutely no material Verizon could remove or access to which it could disable, which suggested that Section 512(c)(3)(A) “concerns means of infringement other than P2P file sharing.”¹⁹²¹

Finally, the court rejected the RIAA’s argument that the definition of “Service Provider” in Section 512(k)(1)(B) made Section 512(h) applicable to an ISP regardless what function it performed with respect to the infringing material – transmission per Section 512(a), caching per Section 512(b), hosting per Section 512(c), or locating it per Section 512(d).¹⁹²² The court stated that this argument “borders upon the silly. ... Define all the world as an ISP if you like, the validity of a § 512(h) subpoena still depends upon the copyright holder having given the ISP, however defined, a notification effective under § 512(c)(3)(A). And as we have seen, any notice to an ISP concerning its activity as a mere conduit does not satisfy the condition of § 512(c)(3)(A)(iii) and is therefore ineffective.”¹⁹²³

The court bolstered its conclusion by pointing to the overall structure of Section 512(h), noting that the presence in Section 512(h) of three separate references to Section 512(c) and the absence of any reference to Section 512(a) suggested the subpoena power of Section 512(h) applies only to ISPs engaged in storing copyrighted material and not to those engaged solely in transmitting it on behalf of others.¹⁹²⁴ The court rejected, however, Verizon’s suggestion that

¹⁹¹⁸ *Id.* at 1235.

¹⁹¹⁹ *Id.*

¹⁹²⁰ *Id.*

¹⁹²¹ *Id.* at 1236.

¹⁹²² *Id.*

¹⁹²³ *Id.*

¹⁹²⁴ *Id.* at 1236-37.

the subpoena power could not apply to ISPs engaged in caching or linking functions under Sections 512(b) and (d). Noting that caching and linking were “storage functions,” the court ruled that “the cross-references to § 512(c)(3) in §§ 512(b)-(d) demonstrate that § 512(h) applies to an ISP storing infringing material on its servers in any capacity – whether as a temporary cache of a web page created by the ISP per § 512(b), as a web site stored on the ISP’s server per § 512(c), or as an information locating tool hosted by the ISP per § 512(d) – and does not apply to an ISP routing infringing material to or from a personal computer owned and used by a subscriber.”¹⁹²⁵

Accordingly, the court remanded the case to the district court with instructions to vacate its order enforcing the RIAA’s subpoena and to grant Verizon’s motion to quash the subpoena.¹⁹²⁶

(3) The Charter Communications Litigation

In Oct. of 2003, Charter Communications filed a motion to quash nearly 150 subpoenas filed by the RIAA as part of its aggressive campaign against peer-to-peer file sharing of music files. Charter challenged the subpoenas on a number of grounds. First, Charter argued that the subpoenas, which demanded compliance within seven days, did not afford a reasonable or feasible time period for Charter to comply with its duties under the federal Cable Communications Act (CCA) to notify subscribers in advance of its compliance. Charter also argued that the CCA allows the turning over of subscribers’ information only where a court order offered evidence that the subscribers were reasonably suspected of engaging in criminal activity, and where the subject of the information had a chance to appear and contest the validity of the claim.¹⁹²⁷

Charter further challenged the subpoenas on the ground that they violated the DMCA by failing to identify the alleged acts of infringement (the subpoenas provided in each case only an e-mail address, date, and time of day, without any identification of copyrighted works that were allegedly infringed), seeking private information beyond the scope of the DMCA, and improperly combining requests for information about 93 different IP addresses into a single subpoena.¹⁹²⁸

The district court issued the subpoenas and denied Charter’s motion to quash. On appeal, the Eighth Circuit reversed.¹⁹²⁹ The court reviewed in detail the logic of the D.C. Circuit’s opinion in the RIAA v. Verizon case and adopted both its reasoning and holding that Section 512(h) does not allow a copyright owner to request a subpoena for an OSP that acts merely as a

¹⁹²⁵ Id. at 1237.

¹⁹²⁶ Id. at 1239.

¹⁹²⁷ “Charter Communications Files Suit, Seeks to Quash RIAA File-Sharing Subpoenas,” *BNA’s Patent, Trademark & Copyright Journal* (Oct. 15, 2003) at 963.

¹⁹²⁸ Id.

¹⁹²⁹ In re Charter Communications, Inc. Subpoena Enforcement Matter, 393 F.3d 771 (8th Cir. 2005).

conduit for data transferred between two Internet users.¹⁹³⁰ The Eighth Circuit did, however, in dicta express certain doubts about the validity of Section 512(h) in general:

For purposes of this appeal, we do not address the constitutional arguments presented by Charter, but do note this court has some concern with the subpoena mechanism of § 512(h). We comment without deciding that this provision *may* unconstitutionally invade the power of the judiciary by creating a statutory framework pursuant to which Congress, via statute, compels a clerk of a court to issue a subpoena, thereby invoking the court's power. Further, we believe Charter has at least a colorable argument that a judicial subpoena is a court order that must be supported by a case or controversy at the time of its issuance. We emphasize, however, for purposes of this appeal we do not reach these issues and have decided this case on the more narrow statutory grounds.¹⁹³¹

(4) **Fatwallet v. Best Buy**

In this case, Fatwallet, Inc. filed a complaint against Best Buy Enterprises, Kohl's Department Stores and Target Corp. seeking declaratory relief related to the alleged unconstitutionality of the subpoena provisions and the notice and takedown provisions of Section 512(c) of the DMCA. The court dismissed the plaintiff's claims in their entirety on grounds of standing. Apparently only Best Buy had issued a subpoena to Fatwallet under the DMCA. The court ruled that Fatwallet did not have standing related to the subpoena because it was undisputed that Best Buy had never attempted to enforce the subpoena. Even if Best Buy had sought to enforce the subpoena, the court noted that it was difficult to see the harm that would befall Fatwallet as opposed to its subscribers, and the subscribers' interest in maintaining their anonymity was insufficient to invoke standing to a third party such as an ISP to challenge the subpoena when the ISP had not suffered an injury of its own. The court distinguished the Verizon decision on the ground that in that case, Verizon had refused to comply with the subpoena and there was a motion to compel, and in any event, the court disagreed with the Verizon decision. The court also ruled that Fatwallet had no standing to assert challenges to the notice and takedown provisions of Section 512(c), because Fatwallet was suffering no injury as a result of those provisions. Because the provisions afford only a positive benefit (a safe harbor from liability), Fatwallet was free to ignore them and no harm would befall it that did not already exist irrespective of the DMCA.¹⁹³²

(5) **In re Subpoena to University of North Carolina at Chapel Hill**

The case of In re Subpoena to University of North Carolina at Chapel Hill¹⁹³³ followed the logic of the RIAA v. Verizon and Charter Communications cases and ruled that Section 512(h) does not allow a copyright owner to obtain a subpoena for an OSP that acts merely as a conduit

¹⁹³⁰ Id. at 776-77.

¹⁹³¹ Id. at 777-78.

¹⁹³² Fatwallet, Inc. v. Best Buy, No. 03 C 50508 (April 12, 2004) (memorandum opinion).

¹⁹³³ 367 F. Supp. 2d 945 (M.D.N.C. 2005).

for data transfer.¹⁹³⁴ In addition, the court rejected the RIAA's argument, as did the courts in the Massachusetts Institute of Technology v. RIAA and Boston College v. RIAA cases discussed in Section II.G.6(h)(1) above, that Section 512(h) allows a party to seek a subpoena in any court in the nation for service in any other district. The court noted authority that the subpoena power of a court cannot be more extensive than its jurisdiction, and that Fed. R. Civ. Pro. 45(b)(2) applies only when a court action or other proceeding is preexisting, which is typically not the case when the subpoena power of Section 512(h) is invoked. Accordingly, the Section 512(h) subpoena must be issued by a court in the district in which the subpoena will be served.¹⁹³⁵

(6) Subpoenas in John Doe Actions

In the wake of the rulings in the RIAA v. Verizon and Charter Communications litigations, copyright owners have turned to filing "John Doe" actions in order to seek subpoenas against OSPs who are mere conduits, and have had success in obtaining subpoenas requiring disclosure of information about subscribers allegedly engaged in copyright infringement through the OSP's service.

For example, in Elektra Entertainment Group, Inc. v. Does 1-6, the court allowed the plaintiffs to take immediate discovery on the University of Pennsylvania to obtain the identity of each Doe defendant by serving a Rule 45 subpoena seeking the name, address, telephone number, email address, and Media Access Control (MAC) address for each defendant. The court required, however, that the Rule 45 subpoena instruct the University of Pennsylvania to distribute a copy of a notice specified by the court to each Doe defendant within seven days of service of the subpoena. The notice informed each defendant that a subpoena disclosing the defendant's identity had been sought and that his or her name had not yet been disclosed, but would be within 21 days if he or she did not challenge the subpoena. The notice contained a list of legal resources who might be able to help the defendant fight the subpoena. The notice further informed the defendant that if he or she did not live or work in Pennsylvania, or visit the state regularly, he or she might be able to challenge the Pennsylvania court's jurisdiction over him or her. Finally, the notice informed the defendant that the record companies were willing to discuss the possible settlement of their claims with the defendant, that the parties might be able to reach a settlement agreement without the defendant's name appearing on the public record, that the defendant might be asked to disclose his or her identity to the record companies if he or sought to pursue settlement, and that defendants who sought to settle at the beginning of a case might be offered more favorable terms by the record companies.¹⁹³⁶

In Strike 3 Holdings, LLC v. Doe,¹⁹³⁷ the district court reversed a magistrate judge's finding of a conflict among the DMCA, the Communications Act, 47 USC § 551, and Rule 45. Specifically,

¹⁹³⁴ Id. at 952-56.

¹⁹³⁵ Id. at 956-58.

¹⁹³⁶ Order, Elektra Entertainment Group, Inc. v. Does 1-6, Civ. Action No. 04-1241 (Oct. 13, 2004). The language of the court's order, without the notice attached, may be found at 2004 U.S. Dist. LEXIS 22673.

¹⁹³⁷ 2019 U.S. Dist. LEXIS 357 (D. Minn. Jan. 2, 2019).

the magistrate judge found that because the information the plaintiff sought in discovery was protected under the Communications Act, it would be improper to subpoena the information under Rule 45. The district court rejected this ruling, finding that because the DMCA establishes a process for copyright holders to obtain subpoenas without engaging in litigation, and the Communications Act provides for disclosure of ISP subscribers' protected information by court order, there is no conflict between those statutes and a Rule 45 subpoena. The court further found that the privacy protections of the Communications Act also do not foreclose a Rule 45 subpoena because Section 551(c)(2)(B) of the Communications Act expressly allows disclosure through a court-ordered subpoena.¹⁹³⁸

In Baughner v. GoDaddy.com LLC,¹⁹³⁹ a group of online bloggers posted certain of the plaintiff's images and work on their blog without permission for the purpose of inviting criticism of it. The plaintiff sent a DMCA takedown notice to GoDaddy.com, which removed the accused blog posts without any counter-notification from the bloggers. The plaintiff then filed an application with the court for a Section 512(h) subpoena to uncover the identities of the Doe bloggers. The Does filed a motion to quash, arguing that the court should look behind the plaintiff's attestation of good faith belief that the Does' use of the plaintiff's work and images infringed her copyright and examine whether the Does' use was fair use and thus not infringing. The Does also argued that disclosure of their identities in compliance with the subpoena would violate their First Amendment right to speak anonymously.¹⁹⁴⁰

The court ruled that, where the target of a Section 512(h) subpoena raises First Amendment concerns about the right to make anonymous speech, the plaintiff must demonstrate a prima facie case of copyright infringement, not just an attestation of a good faith belief under Sections 512(c)(3)(A), (h)(1) and (h)(2), and the court must then conduct a balancing of harms under Fed. R. Civ. Pro. 45 in deciding a motion to quash. Here, the plaintiff had copyright registrations in 20 of the 22 photos posted, which constituted prima facie evidence of copyright validity for those 20 photos, and the Does had not raised any meritorious legal challenges to the plaintiff's copyrights in the work and images they allegedly posted on their blog. Nor had the Does pointed to any evidence that they did not reproduce the plaintiff's work and images on the blog. In addition, the court ruled the Does had not shown that their postings were a fair use. The postings were done without substantial comment or criticism and therefore were not transformative, and the Does had proffered no evidence to show their use had no effect on the value of the posted works. In sum, because the plaintiff had successfully demonstrated a prima facie claim of copyright infringement and the Does had not demonstrated fair use, the Does had little, if any First Amendment protection against disclosure of their identities. The court there denied the motion to quash the subpoena.¹⁹⁴¹

¹⁹³⁸ Id. at *4-7.

¹⁹³⁹ Baughner v. GoDaddy.com, Inc., 2021 U.S. Dist. LEXIS 204449 (D. Ariz. Oct. 22, 2021).

¹⁹⁴⁰ Id. at *1-3.

¹⁹⁴¹ Id. at *5-14.

(7) Interscope Records v. Does 1-7

In Interscope Records v. Does 1-7,¹⁹⁴² the court followed the Charter Communications and Verizon cases in holding that Section 512(h) does not authorize the issuance of subpoenas against Section 512(a) OSPs who act merely as conduits.¹⁹⁴³ The plaintiffs had sought such a subpoena against the College of William and Mary, which provided Internet services that the Doe defendants allegedly used to access a peer-to-peer online media distribution system for the purpose of downloading and distributing plaintiffs' copyrighted works.¹⁹⁴⁴

(8) In re Maximized Living

In In re Maximized Living, Inc. v. Google, Inc.,¹⁹⁴⁵ the court ruled that the subpoena power of Section 512(h) is limited to currently infringing activity and does not reach former infringing activity that has ceased and can thus no longer be removed or disabled. In this case, because Google had already taken down the plaintiff's copyrighted scripts from an Internet blog hosted by Google, the use of a Section 512(h) subpoena to still seek to obtain the identity of the user who had posted those scripts was invalid.¹⁹⁴⁶

(9) In re Subpoena Issued to Birch Communications

In In re Subpoena Issued to Birch Communications,¹⁹⁴⁷ a magistrate judge, adjudicating the issue as one of first impression in the Eleventh Circuit, quashed a subpoena by Rightscorp, Inc. issued to an ISP seeking the name, address, telephone number and email address of more than 1,000 of the ISP's customer that were identified by IP addresses in an attachment to the subpoena. The court found the reasoning of the RIAA v. Verizon and In re Charter Communications cases persuasive for the rule that Section 512(h) subpoenas may not be issued to service providers that act only as a conduit for data transferred between other parties and that do not store data.¹⁹⁴⁸ Rightscorp appealed the ruling to the district court, which affirmed the magistrate's ruling on the same rationale. The court found the opinions in RIAA v. Verizon and In re Charter Communications persuasive. Because the ISP did not store or host on its servers the allegedly infringing material, there was no allegedly infringing material to be removed or access disabled. Because Rightscorp therefore could not satisfy the notice requirements of Section 512(c)(3)(A), which is a prerequisite to issuance of a subpoena under

¹⁹⁴² 494 F. Supp. 2d 388 (E.D. Va. 2007).

¹⁹⁴³ Id. at 388.

¹⁹⁴⁴ Id.

¹⁹⁴⁵ 2011 U.S. Dist. LEXIS 147486 (N.D. Cal. Dec. 22, 2011).

¹⁹⁴⁶ Id. at *3-4, *13-16.

¹⁹⁴⁷ Order, In re Subpoena Issued to Birch Communications, Inc., Civil Action File No. 1:14-CV-03904-WSD-JFK (N.D. Ga. Jan. 16, 2015).

¹⁹⁴⁸ Id. at pp. 3-6.

Section 512(h), a subpoena could not be issued under Section 512(h).¹⁹⁴⁹ In a footnote, the court noted the alternative available to Rightscorp to a Section 512(h) subpoena would be to bring a *John Doe* action and seek a subpoena pursuant to F.R.C.P. 45.¹⁹⁵⁰

(10) In re DMCA Subpoena Issued to eBay, Inc.

In this case, the court rejected eBay's challenge to a Section 512(h) subpoena on the ground that no infringing activity was occurring on eBay's servers at the time the subpoena was served because eBay had already taken down the allegedly infringing material in response to DMCA takedown notices sent by petitioner Barry Rosen. The magistrate judge ruled that, so long as allegedly infringing material was present on eBay's servers at the time the takedown notices were sent to eBay that formed the basis for the Section 512(h) subpoena, eBay must respond to the subpoena.¹⁹⁵¹ As support for its conclusion, the court pointed to language in Section 512(h)(5) stating that upon receipt of the subpoena the service provider must expeditiously disclose the information required by the subpoena "regardless of whether the service provider responds to the notification."¹⁹⁵² The court thus concluded that a Section 512(h) subpoena is valued whether served simultaneously with a satisfactory DMCA notification or after a satisfactory DMCA notification is served.¹⁹⁵³

The court also ruled, however, that the subpoena at issue was overbroad by calling for disclosure of "all identifying information" for each of 61 user names submitted who had posted allegedly infringing items on eBay from the time their accounts were established to the present. The court concluded that it was necessary only for eBay to produce from its records information sufficient to identify the alleged infringers, and therefore ordered eBay to produce to Rosen only the name, last known address, last known telephone number, any electronic mail addresses associated with each account, and any logs of IP addresses used to access the subject accounts from the time the accounts were established up to the date of the subpoena.¹⁹⁵⁴

(11) In re DMCA Subpoena to Reddit, Inc.

This case held that a Section 512(h) subpoena is invalid against a user who is making a fair use of a work, as he is not an infringer at all and Section 512(h) may be used only to discover the identity of an alleged infringer. A pseudonymous user of Reddit sought district court review of a magistrate judge's decision denying his motion to quash a subpoena issued under Section 512(h) by The Watch Tower Bible and Tract Society of Pennsylvania to uncover the user's

¹⁹⁴⁹ In re Subpoena Issued to Birch Communications, Inc., 2015 U.S. Dist. LEXIS 58485 at * 14-16 (N.D. Ga. May 5, 2015).

¹⁹⁵⁰ Id. at *17 n.11.

¹⁹⁵¹ In re DMCA Subpoena to eBay, Inc., 2015 U.S. Dist. LEXIS 73341 at * 5-8 (S.D. Cal. June 5, 2015).

¹⁹⁵² Id. at *8.

¹⁹⁵³ Id. at *8-9.

¹⁹⁵⁴ Id. at *9-11.

identity after he posted images of Watch Tower documents to criticize its fundraising and data collection practices. The district court agreed that the subpoena should be quashed. Under the Ninth Circuit’s ruling in Lenz (discussed in Section III.C.6(b)(4)(vi) below), fair use is not just excused by the law, it is wholly authorized by the law. The court therefore ruled that if the user were to establish that he made fair use of the copyrighted works, no claim of copyright infringement could plausibly be alleged against him, and the subpoena would not be authorized under the DMCA. After a de novo review of the record and the parties’ arguments, the court concluded that the user made fair use of the Watch Tower documents and therefore granted the motion to quash the subpoena.¹⁹⁵⁵

(12) In re DMCA Section 512(h) Subpoena to YouTube (Google, Inc.)

This case arose out of a Section 512(h) subpoena to identify an alleged infringer of copyrights held by Watch Tower Bible and Tract Society of Pennsylvania, an organization that published religious materials for Jehovah’s Witnesses. The movant John Doe, a lapsed Jehovah’s Witness who published satirical videos critical of the religious denomination on YouTube, moved to quash the subpoena. The court cited previous cases holding that if a fair use inquiry demonstrates the movant is not an infringer of the copyrighted works, the subpoena would not be authorized under the DMCA and must be quashed. Here, there was no factual dispute as to facts relevant to the fair use issue, which the court found the movant was entitled to, and the court therefore quashed the subpoena.¹⁹⁵⁶

9. Proposed Limitation of Scope of Shrinkwrap and Clickwrap Licenses That Did Not Pass

H.R. 3048 contained an interesting and potentially controversial provision that would have extended the scope of the preemption provisions of the copyright statute to limit certain provisions common to shrinkwrap and clickwrap license agreements. Specifically, H.R. 3048 would have added the following provision at the end of Section 301(a) of the copyright statute:

When a work is distributed to the public subject to non-negotiable license terms, such terms shall not be enforceable under the common law or statutes of any state to the extent that they –

- (1) limit the reproduction, adaptation, distribution, performance, or display, by means of transmission or otherwise, of material that is uncopyrightable under section 102(b) or otherwise; or
- (2) abrogate or restrict the limitations on exclusive rights specified in sections 107 through 114 and sections 117 and 118 of this title.

¹⁹⁵⁵ In re DMCA Subpoena to Reddit, Inc., 2020 U.S. Dist. LEXIS 37033 at *1, *17-18 & *29 (N.D. Cal. Mar. 2, 2020).

¹⁹⁵⁶ In re DMCA Section 512(h) Subpoena to YouTube (Google, Inc.), 2022 U.S. Dist. LEXIS 9209 at *1, *13-15 & *28 (S.D.N.Y. Jan. 18, 2022).

Clause (1) was apparently intended to establish an affirmative principle that subject matter which is not protected by copyright under Section 102(b) of the copyright statute (which includes “any idea, procedure, process, system, method of operation, concept, principle, or discovery”) cannot be the subject of contractual prohibitions on reproduction, adaptation, distribution, performance or display in a license having non-negotiable terms (such as a shrinkwrap or clickwrap agreement). Although this provision is founded on a philosophical notion that subject matter which the copyright law deems free for the public to use should not be withdrawn from use, at least by virtue of a non-negotiable license, it might have had unintended consequences with respect to confidentiality clauses that protect trade secret material.

Specifically, many shrinkwrap or clickwrap agreements contain confidentiality clauses that prohibit the disclosure, use and reproduction of trade secret subject matter embodied in software that will typically fall within the enumerated subject matter of Section 102(b) of the copyright statute. Clause (1) could have been read to preempt these confidentiality clauses. This seems like a somewhat strange result in view of the Supreme Court’s ruling that copyright law does not preempt state trade secret law.¹⁹⁵⁷ The authors of H.R. 3048 apparently saw a more pernicious effect from such clauses simply because they are contained in a non-negotiable license, although it is not clear why.

Clause (2) would have preempted clauses in a shrinkwrap or clickwrap agreement that have the effect of restricting the limitations on copyright rights enumerated in Sections 107 through 114, 117, and 118 of the copyright statute. This provision would have affected many shrinkwrap and clickwrap agreements in at least two ways. First, because many courts have ruled that disassembly of computer programs to extract ideas from them is a fair use under certain circumstances,¹⁹⁵⁸ the clauses which flatly prohibit disassembly or reverse engineering of software that are common in shrinkwrap and clickwrap agreements might have been preempted. Second, clauses which prohibit transfer of a copy of a computer program by the licensee to a third party (a right that would otherwise be available if the first sale doctrine of Section 109 of the copyright statute is deemed applicable by treating a shrinkwrap license transaction as a sale) might have been preempted.

It is unknown whether there will be efforts to reintroduce this provision in another session of Congress.

¹⁹⁵⁷ Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974).

¹⁹⁵⁸ See Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1993); Atari Games Corp. v. Nintendo of America, Inc., 975 F.2d 832 (Fed. Cir. 1992); DSC Communications Corp. v. DGI Technologies Inc., 898 F. Supp. 1183 (N.D. Tex. 1995).

III. APPLICATION OF COPYRIGHT RIGHTS TO SPECIFIC ACTS ON THE INTERNET

As is apparent from Part II, copyright owners hold a potentially very broad panoply of rights that may be applicable to acts on the Internet. These rights may well be expanded by the WIPO treaties. Part III of this paper analyzes the potential application of such rights to various actions on the Internet, such as browsing, caching, linking, operation of an Internet service or bulletin board, creation of derivative works, and resale or subsequent transfer of works downloaded from the Internet, as well as how various traditional defenses – such as fair use and the implied license doctrine – may be interpreted with respect to Internet activities.

A. Browsing

Browsing is probably the single most common activity of users on the Internet today. It provides a graphic illustration of the difficulty and uncertainty of applying traditional copyright rights, in which tangible objects are the paradigm for transfer of information, to the Internet medium, in which electronic transmissions are the paradigm for transfer of information. The difficulty arises principally from the fact that, unlike in the case of traditional media, reading or use of a copyrighted work on the Internet generally requires making a “copy” of the work (at least under the logic of the MAI case and its progeny and under the WIPO Copyright Treaty), and may require a distribution, transmission, and access of the work as well. Thus, although “reading” and “using” are not within a copyright holder’s exclusive rights, copying, distribution, and (under the WIPO treaties) transmission and access, are. To the extent the latter acts are necessarily incidental to browsing a work on the Internet, such browsing may technically infringe multiple rights of the copyright holder.

Indeed, one decision held that the act of browsing an unauthorized copy of a copyrighted work constituted copyright infringement, because the browsing caused an additional copy of the work to be made in RAM. Specifically, in Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.,¹⁹⁵⁹ the court, citing the MAI decision, stated, “When a person browses a website, and by so doing displays the [copyrighted material], a copy of the [copyrighted material] is made in the computer’s random access memory (RAM), to permit viewing of the material. And in making a copy, even a temporary one, the person who browsed infringes the copyright.”¹⁹⁶⁰

In addition, browsing may implicate the right of public display and/or public performance. For example, the NII White Paper takes the position that browsing through copies of works on the Internet is a public display of at least a portion of the browsed work.¹⁹⁶¹ In addition, at least isochronous downloading of performances of copyrighted works in the course of browsing by members of the public, such as from a commercial online service like America On Line (AOL),

¹⁹⁵⁹ 53 U.S.P.Q.2d 1425 (D. Utah 1999).

¹⁹⁶⁰ Id. at 1428.

¹⁹⁶¹ NII White Paper at 45.

may constitute infringements of the public performance right.¹⁹⁶² As noted in Part II above, the fact that potential recipients of transmitted displays and performances are geographically and/or temporally dispersed does not prevent a transmission to a single recipient in any given instance from creating a “public” display or performance.

In a great many instances, a copyright holder will have placed material on the Internet with the intent and desire that it be browsed. Browsing of such material will no doubt be deemed to be either within the scope of an implied license from the copyright holder or a fair use. For example, the court in Religious Technology Center v. Netcom On-Line Communication Services¹⁹⁶³ noted in dicta that much of digital browsing is probably a fair use or an innocent infringement:

Absent a commercial or profit-depriving use, digital browsing is probably a fair use; there could hardly be a market for licensing the temporary copying of digital works onto computer screens to allow browsing. Unless such a use is commercial, such as where someone reads a copyrighted work online and therefore decides not to purchase a copy from the copyright owner, fair use is likely. Until reading a work online becomes as easy and convenient as reading a paperback, copyright owners do not have much to fear from digital browsing and there will not likely be much market effect.

Additionally, unless a user has reason to know, such as from the title of a message, that the message contains copyrighted materials, the browser will be protected by the innocent infringer doctrine, which allows the court to award no damages in appropriate circumstances. In any event, users should hardly worry about a finding of direct infringement: it seems highly unlikely from a practical matter that a copyright owner could prove such infringement or would want to sue such an individual.¹⁹⁶⁴

Although the Netcom court is no doubt correct in its observations under U.S. copyright law, nevertheless browsing raises important copyright problems that cannot be dismissed simply on the notion that doctrines such as fair use, implied license, or innocent infringement will remove the problems entirely. First, Internet activities are inherently global, and countries outside the U.S. may not apply defensive doctrines such as fair use and implied license as broadly as U.S. courts. At best, the rules may differ from country to country, which will breed uncertainty and the possibility of inconsistent results in different countries.

Second, as elaborated below in the discussion on caching, copyright owners may begin placing notices on their works governing the uses to which they may be put. Such notices may restrict use of the work in ways that are unclear or undesirable, and the applicability of the fair use or implied license doctrines may become more uncertain in the face of such notices.

¹⁹⁶² The public digital performance right in a sound recording may also be implicated.

¹⁹⁶³ 907 F. Supp. 1361 (N.D. Cal. 1995).

¹⁹⁶⁴ Id. at 1378 n.25.

Third, the fact that browsing, an activity akin to reading in traditional media, potentially constitutes literal infringement of so many copyright rights represents a significant shift in the balance between the rights of purchasers and users on the one hand, and the interests of copyright owners on the other. As one commentator stated:

The conflict here of perspective, policy, and technology may be a defining issue in cyberspace. ... [T]he idea that reading a digital text entails a potential copyright violation shifts policy. That shift, even if desirable, should occur because of an express policy choice rather than because new technology technically triggers concepts originally designed for a world of photocopy machines, recorders, and the like.¹⁹⁶⁵

Such policy shift, and the details of it, may not be expressly defined in U.S. copyright law (and perhaps in the copyright laws of other countries as well) until legislation implementing the WIPO treaties is considered.

B. Caching

Caching is another activity that is, under current technology, virtually ubiquitous on the Internet. Caching (sometimes known as “mirroring,” usually when it involves storage of an entire site or other complete set of material from a source) means storing copies of material from an original source site (such as a Web page) for later use when the same material is requested again, thereby obviating the need to go back to the original source for the material. The purpose of caching is to speed up repeated access to data and to reduce network congestion resulting from repeated downloads of data. The cached material is generally stored at a site that is geographically closer to the user, or on a more powerful computer or one that has a less congested data path to the ultimate user. The cached information is usually stored only temporarily, although the times may vary from a few seconds to a few days, weeks, or more.

1. Types of Caching

Caching may be of the following types:

- Local Caching: Caching generally occurs locally at the end user’s computer, either in RAM, on the hard disk, or some combination of both. Most browsers, for example, store recently visited Web pages in RAM or on the hard disk. When the user hits the “Back” key, for example, the browser will usually retrieve the previous page from the cache, rather than downloading the page again from the original site. This retrieval from cache is much faster and avoids burdening the network with an additional download.
- Proxy Caching: Proxy caching occurs at the server level, rather than at the end user’s computer level. Specifically, a copy of material from an original source is stored on a server other than the original server. For example, an OSP such as AOL may store on its own server for a certain period of time Web pages that have been previously requested

¹⁹⁶⁵ R. Nimmer, Information Law ¶ 4.08[1], at 4-30 (2001).

by AOL users. When another user subsequently requests a page previously stored, AOL may download the page from its own server, rather than fetching the page from the original source server.

The use of caching on the Internet stems from at least three reasons: to overcome transmission bandwidth limitations, to load balance serving up web pages (such as through search engines) or distributing other content in high demand through multiple sources, and to preserve archival versions of web pages for use in the event that web sites are removed or go down temporarily.

Caching presents difficult copyright issues on a number of fronts. Because caching involves the making of copies, it presents an obvious problem of potential infringement of the right of reproduction. In addition, proxy caching may give rise to infringement of the rights of public distribution, public display, public performance, and digital performance, since copies of copyrighted works may be further distributed and displayed or performed from the cache server to members of the public. Under the WIPO treaties, caching may also infringe the new rights of transmission and access. Because the situs of infringements of these rights under the WIPO treaties is most likely the server, caching may give rise to infringements at every proxy server. Large OSPs may have proxy servers at many sites around the globe.

2. The Detriments of Caching

From a legal perspective, because caching has obvious technical benefits in getting information from the Internet to a user faster, one might assume that a copyright owner who has placed information on the Internet and desires such information to reach end users as expeditiously as possible would have no incentive to assert its copyright rights against caching.¹⁹⁶⁶ In legal terms, one might be tempted to conclude that caching will fall within the fair use or implied license doctrines. However, the legal analysis is complex, because caching carries with it a number of potential detriments to the owner of the copyrighted material:¹⁹⁶⁷

- Loss of Version Control: Caching interferes with the ability of a website operator to control what version of information is delivered to the end user.¹⁹⁶⁸ For example, a website may have been substantially improved, yet an old version of material from the site may reside on the proxy server of the end user's OSP. Many end users may therefore not see the improved version the website owner desired to present to the public. In a more serious vein, suppose a website owner is notified that its site contains infringing or defamatory material. To avoid liability, the website owner may remove such material

¹⁹⁶⁶ Indeed, in a poll taken during 1997 by *Interactive PR & Marketing News*, 82% of respondents answered "no" to the question, "Do you feel that caching of content of Web sites or online service providers constitutes infringement?" *Interactive PR & Marketing News*, Vol. 4, No. 28 (Aug. 8, 1997), at 1.

¹⁹⁶⁷ In addition to the detriments noted to the copyright owner, caching can give rise to potential liability on the part of the caching entity. For example, if an original site contains defamatory material, the caching entity may be deemed to have "republished" that defamatory information through the caching mechanism.

¹⁹⁶⁸ Eric Schlachter, "Caching on the Internet," *Cyberspace Lawyer*, Oct. 1996, at 2, 3.

promptly, yet it may continue to be distributed through old cached versions, giving rise to potential ongoing liability.

- Out of Date Information: Many websites may contain time sensitive information, such as stock quotes or sports scores. If information is obtained from a cache rather than the original site, and the cache has not been refreshed recently, the user may obtain out of date information or information that is no longer accurate. The problem is heightened by the fact that most caching is “invisible” to the user. In many instances the user will simply not know whether the information being presented is cached information, how recently the cache was refreshed, or whether the information contained in the cached version is now out of date as compared to information at the original site. A user may therefore unknowingly rely on inaccurate information to his or her detriment.
- Interference with Timed Information: Closely related to the problem of out of date information is the problem of interference with timed information. For example, a website owner may have contracted with an advertiser to display an advertising banner during a certain window of time, say 7:00 to 8:00 p.m. If a page from the site is downloaded into a cache at 7:30 p.m. and is not refreshed for several hours, users will see the ad for far more than the one hour the advertiser paid for, and may not see at all the ad that the next advertiser paid to have displayed from 8:00 p.m. to 9:00 p.m.¹⁹⁶⁹
- Inaccurate Page Impression and Other Information: Many websites keep track of the number of “page impressions” at the site – i.e., the number of times a page is displayed from the site to users. Page impressions are often used as a measure for advertising charges – the more page impressions a site generates among users, the more the site can charge for advertisements placed on the site. Accesses to cached versions of a Web page may not be counted as page impressions at the original site,¹⁹⁷⁰ and the original website owner may not know how often a given page was viewed from the cache.¹⁹⁷¹ Reduced page impression counts cost the website owner advertising revenues. In addition, many sites maintain “server logs” which record activities of users of the site, from which valuable information may be gleaned. Accesses to cached information will generate entries into the logs of the proxy server, not the original site.
- Loss of Limits on Access: Caching may also result in the loss of control over access to information at a site. For example, suppose a website owner desires to limit access to material on a site to a single user at a particular institution through use of a password.

¹⁹⁶⁹ See *id.* at 3.

¹⁹⁷⁰ David G. Post, “Bargaining in the Shadow of the Code: File Caching, Copyright, and Contracts Evolving in Cyberspace,” at 7 (paper presented at the University of Dayton School of Law Symposium on “Copyright Owners’ Rights and Users’ Privileges on the Internet,” Nov. 1-2, 1996; copy on file with the author).

¹⁹⁷¹ At least one online service markets to website owners data about the number of page impressions delivered from its cache. Schlachter, *supra* note 1958, at 3.

Such user could enter the password, download the information to a proxy server, and then other, unauthorized users might be able to gain access to it.¹⁹⁷²

As discussed in detail in Section III.C below, the DMCA creates a safe harbor for caching by OSPs under defined circumstances, which in part anticipate, and condition the safe harbor upon, compliance with technical solutions that may develop and become industry standards. The safe harbor implicitly recognizes, and seems designed to minimize, the potential detriments of caching discussed above.

3. The Netcom Case and Application of the Fair Use Doctrine

As discussed in detail in Section III.C.6(b)(1)(ii) below, the DMCA creates a safe harbor for caching by OSPs under defined circumstances. Even if the conditions required under the DMCA are not met to take advantage of the safe harbor, a person performing caching of copyrighted material might nevertheless seek to justify it under either the fair use or implied license doctrines. Because of the potential detriments of caching, application of the fair use and implied license doctrines to caching is uncertain.

This subsection gives a general analysis of the legal issues that arise in applying the fair use doctrine to caching, from the perspective of an OSP performing proxy caching, since OSPs or similar entities seem the most likely targets for claims of infringement by copyright owners based on caching.¹⁹⁷³ The analysis uses as a springboard the first case to address the applicability of the fair use doctrine to an OSP in a factual setting akin to caching, Religious Technology Center v. Netcom On-Line Communication Services.¹⁹⁷⁴ Subsection 4 below discusses other cases since Netcom that have expressly adjudicated the application of the fair use and implied license doctrines to caching. In the Netcom case, the plaintiff sought to hold Netcom, an OSP, liable for allegedly infringing material that was “mirrored” on its server as part of providing Usenet news group services to its subscribers. The holding of that case with respect to the various fair use factors is analyzed below.

(a) Purpose and Character of the Use

The first statutory fair use factor looks to the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes. Proxy caching is generally done in the context of providing commercial services to end users, and is therefore likely to be for a commercial purpose. However, the Netcom court noted that Netcom’s use of copyrighted material as part of its Usenet services, “though commercial, also benefits the public in allowing for the functioning of the Internet and the dissemination of other

¹⁹⁷² Post, supra note 1970, at 8.

¹⁹⁷³ One commentator argues that even local caching might give rise to suit by a copyright owner: “For example, such a suit might arise in the case of a large company where the cumulative effects of local caching by many Web browsers (perhaps combined with statutory damages and attorneys fees) are significant.” Schlachter, supra note 1958, at 4.

¹⁹⁷⁴ 907 F. Supp. 1361 (N.D. Cal. 1995).

creative works, a goal of the Copyright Act.”¹⁹⁷⁵ The court noted that the commercial nature of Netcom’s activity should therefore not be dispositive, concluding that “[b]ecause Netcom’s use of copyrighted materials served a completely different function than that of the plaintiffs, this factor weighs in Netcom’s favor.”¹⁹⁷⁶

In many instances, however, it may be unclear whether an OSP’s particular form of caching serves a “completely different function” than that of the copyright owner’s use of its material. For example, material may be cached from a source website and accessed by users from the proxy server in exactly the same way that it would have been accessed from the original server. The copyright holder might use this fact to distinguish the Netcom court’s holding with respect to the first statutory fair use factor.

(b) Nature of the Copyrighted Work

The second statutory fair use factor looks to the nature of the copyrighted work. Fair use rights are generally construed more broadly with respect to factual or published works than with respect to fictional or unpublished works. Although all material available on the Internet is published, such material varies tremendously as to its substantive nature. Thus, whether a particular cached work is factual, fictional, or in between, will vary from case to case, and the application of the second statutory factor to any particular instance of caching cannot necessarily be predicted in advance.

In the Netcom case, the court held that the precise nature of the works at issue was not important to the fair use determination “because Netcom’s use of the works was merely to facilitate their posting to the Usenet, which is an entirely different purpose than plaintiffs’ use.”¹⁹⁷⁷ As noted with respect to the first statutory fair use factor, however, the same may often not be true in particular instances of caching. Accordingly, it is difficult to say how the second statutory factor may be applied to caching in particular instances.

(c) Amount and Substantiality of the Portion Used

The third statutory fair use factor looks to the amount and substantiality of the portion used in relation to the copyrighted work as a whole. Caching routinely involves the making of copies of entire Web pages, which may in turn contain entire copyrighted works,¹⁹⁷⁸ so in many instances all or a substantial portion of a copyrighted work will be copied in the course of caching. Generally, no more of a work may be copied than is necessary for the particular use.¹⁹⁷⁹

¹⁹⁷⁵ Id. at 1379.

¹⁹⁷⁶ Id.

¹⁹⁷⁷ Id.

¹⁹⁷⁸ Schlachter, supra note 1958, at 4.

¹⁹⁷⁹ See, e.g., Supermarket of Homes v. San Fernando Valley Board of Realtors, 786 F.2d 1400, 1409 (9th Cir. 1986).

Although copying an entire work will ordinarily militate against a finding of fair use,¹⁹⁸⁰ one could argue that caching inherently requires copying all or a substantial portion of the cached material in order to derive the benefits of the caching, and this factor should therefore not be dispositive of fair use.

For example, the Netcom court noted that “the mere fact that all of a work is copied is not determinative of the fair use question, where such total copying is essential given the purpose of the copying.”¹⁹⁸¹ Because Netcom had copied no more of the plaintiff’s works than necessary to function as a Usenet server, the court concluded that the third statutory factor should not defeat an otherwise valid defense.¹⁹⁸²

OSPs that engage in copying of whole works may be able to rely on this logic by arguing that such copying is essential given the nature and purpose of caching. Such an argument may, however, be vulnerable to attack, depending upon the way in which the caching is performed. Caching by an OSP of only that material that has been requested by users in some previously defined time period may be said to be “essential” because such material has at least a demonstrated basis for expecting that it will be accessed again. But what about extensive “mirroring,” where an OSP copies, for example, entire websites from geographically remote sites to more local servers? Such caching is not based on actual demand usage. Should this matter? Could the OSP argue that such caching is “essential” to avoid potential network bottlenecks from the remote site to its users’ computers? The case of Field v. Google, discussed in Section III.B.4(a) below, found extensive caching by Google using automated robots to be a fair use.

(d) Effect of Use on the Potential Market

The fourth statutory fair use factor looks to the effect of the use upon the potential market for or value of the copyrighted work. This factor is generally considered the most important of the four factors.¹⁹⁸³ In analyzing this factor, a court may look to “whether unrestricted and widespread conduct of the sort engaged in by the defendant ... would result in a substantially adverse impact on the potential market’ for the original.”¹⁹⁸⁴ Because caching is inherently widespread on the Internet, a court may well look beyond the individual actions of a particular caching entity and assess the potential aggregate impact of caching on a copyright owner.

¹⁹⁸⁰ Sony Corp. v. Universal Studios, Inc., 464 U.S. 417, 449-50 (1984).

¹⁹⁸¹ Netcom, 907 F. Supp. at 1380 (citing the Supreme Court’s decision in Sony, in which the Court held that total copying of copyrighted broadcast programs for the purpose of time-shifted viewing was a fair use).

¹⁹⁸² Netcom, 907 F. Supp. at 1380.

¹⁹⁸³ See 4 M. Nimmer & D. Nimmer, *Nimmer on Copyright* § 13.05[A][4], at 13-180 to –181 (1999) (citing, inter alia, Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 566 (1985)).

¹⁹⁸⁴ Campbell v. Acuff-Rose Music, Inc., 114 S. Ct. 1164, 1177 (1994) (quoting 3 M. Nimmer & D. Nimmer, *Nimmer on Copyright* § 13.05[A][4]).

The application of this factor is very difficult to predict in advance, without knowing the particular factual circumstances of the caching that is being challenged. There are no doubt many instances of caching that do not harm the potential market for a copyright owner's work, especially with respect to caching of material from non-commercial websites that make material available for free. However, even in the case of non-commercial sites, one or more of the detriments of caching noted in subsection 2 above may be applicable, and the copyright owner might use such detriments as the basis for an argument of harm to the potential market for the copyrighted material. For example, a website owner might put promotional material up on its site that is updated frequently. If caching caused the latest updated material not to be available, the owner might argue that the "market" for its website material had been harmed.

With respect to commercial sites, one can more readily imagine instances in which caching could cause harm to the market for copyrighted works. For example, if caching reduces the number of page impressions generated by a home page containing copyrighted material on which advertising is sold, the owner could argue that its advertising revenues for ads placed in conjunction with such copyrighted material (which, in this instance, is arguably the very "market" for such material) will be harmed.

In the Netcom case, the court held that potential harm under the fourth fair use factor precluded a ruling that the OSP's posting of the plaintiffs' copyrighted material in its Usenet service was a fair use. The plaintiffs had argued that the Internet's extremely widespread distribution of its copyrighted religious materials multiplied the potential effects of market substitution for its materials by groups using such materials to charge for Scientology-like religious training.¹⁹⁸⁵

In sum, it seems that the application of the fourth fair use factor will be highly fact specific, and there may be instances in which a copyright holder could establish sufficient harm to its potential markets from caching as to preclude a finding of fair use. It therefore seems unwise to make a blanket assumption that the fair use doctrine will automatically protect all forms of caching.

The potential harm to copyright owners from caching also introduces uncertainty with respect to whether the implied license doctrine may apply to caching in various instances. Courts often tend to construe implied licenses narrowly.¹⁹⁸⁶ A court might therefore be hesitant

¹⁹⁸⁵ Netcom, 907 F. Supp. at 1380.

¹⁹⁸⁶ See, e.g., MacLean Assocs. Inc. v. Wm. M. Mercer-Meidinger-Hansen Inc., 952 F.2d 769 (3d Cir. 1991) (defendant obtained an implied license to use a computer program prepared by an independent contractor, but only in the furtherance of its business relationship with one particular client for which the contractor had been engaged to support); Oddo v. Reis, 743 F.2d 630 (9th Cir. 1984) (scope of implied license included the right to market an unmodified computer program to third parties, subject to an obligation to account for profits to the developer, but did not include a right to modify); see also Microstar v. Formgen, Inc., 942 F. Supp. 1312, 1318 (S.D. Cal. 1996); Meadows, "Practical Aspects of 'Implied License,'" *Computer Law Strategist* (May 1993) at 1. See generally Barry & Kothari, "Other People's Property: There May Be Implied Licenses for Content on Web Pages," *San Francisco Daily Journal* (Aug. 28, 1997) at 5.

to construe any implied license from a copyright owner based on its posting of material for browsing on the Web to cover uses (such as caching) that cause palpable harm to the owner.

4. Cases Adjudicating Caching Under the Fair Use and Implied License Doctrines

(a) *Field v. Google*

In *Field v. Google*¹⁹⁸⁷ the plaintiff, Field, alleged that by allowing Internet users to access copies of his copyrighted works stored by Google in its online cache, Google was violating his exclusive rights to reproduce and distribute copies of those works. The court ruled that Google's acts were covered by the fair use and implied license doctrines.

The challenged acts arose in the context of Google's search engine and its accompanying Web crawler, the Googlebot. The Googlebot automatically and continuously crawled the Internet to locate and analyze Web pages and to catalog those pages into Google's searchable Web index. As part of the process, Google made and analyzed a copy of each Web page the Googlebot found and stored the HTML code from those pages in a cache so as to enable those pages to be included in the search results displayed to users in response to search queries. When Google displayed Web pages in its search results, the first item appearing was the title of a Web page which, if clicked, would take the user to the online location of that page. The title was followed by a short snippet of text from the Web page in a smaller font. Following the snippet, Google typically provided the full URL for the page. Then, in the same smaller font, Google often displayed another link labeled "Cached." When clicked, the "Cached" link directed a user to the archival copy of a Web page stored in Google's system cache, rather than to the original Web site for that page. By clicking on the "Cached" link for a page, a user could view the snapshot of that page as it appeared the last time the site was visited and analyzed by the Googlebot.¹⁹⁸⁸

The court noted that Google provided "Cached" links for three principal reasons – to allow viewing of archival copies of pages that had become inaccessible because of transmission problems, censorship, or because too many users were trying to access the content at a particular time; to enable users to make Web page comparisons to determine how a particular page had been altered over time; and to enable users to determine the relevance of a page by highlighting where the user's search terms appeared on the cached copy of the page.¹⁹⁸⁹

Of particular relevance to the court's rulings were certain widely recognized and well publicized standard protocols that the Internet industry had developed by which Web site owners could automatically communicate their preferences to search engines such as Google. The first mechanism was the placement of meta-tags within the HTML code comprising a given page to instruct automated crawlers and robots whether or not the page should be indexed or cached. For example, a "NOINDEX" tag would indicate an instruction that the Web page in which

¹⁹⁸⁷ 412 F. Supp. 2d 1106 (D. Nev. 2006).

¹⁹⁸⁸ *Id.* at 1110-11.

¹⁹⁸⁹ *Id.* at 1111-12.

it was embedded should not be indexed into a search engine, and a “NOARCHIVE” tag would indicate that the page should not be cached or archived. When the Googlebot visited a page, it would search for meta-tags in the HTML of the page and obey them.¹⁹⁹⁰

The second mechanism by which Web site owners could communicate with search engines’ robots was by placing a “robots.txt” file on the Web site containing textual instructions concerning whether crawling of the site was allowed. If the Googlebot encountered a robots.txt file with a command disallowing crawling, it would not crawl the Web site, and there would therefore be no entries for that Web site in Google’s search results and no “Cached” links. The court noted that the Internet industry had widely recognized the robots.txt file as a standard for controlling automated access to Web pages since 1994.¹⁹⁹¹

In the court’s words, Field decided to “manufacture a claim for copyright infringement against Google in the hopes of making money from Google’s standard practice”¹⁹⁹² of caching by placing his copyrighted works on a Web site available to the public for free and creating a robots.txt file on the site with the permissions set within the file to *allow* all robots to visit and index all of the pages on the site, knowing that this would cause the Googlebot to cache his copyrighted works. Field testified in his deposition that he had consciously chosen not to use the NOARCHIVE meta-tag on his Web site. When Google learned that Field had filed (but not served) a complaint for copyright infringement, Google promptly removed the “Cached” links to all of the pages on his site.¹⁹⁹³

Field alleged only claims of direct copyright infringement against Google (and made no claims for contributory or vicarious liability), asserting that Google directly infringed his copyrights when a Google user clicked on a “Cached” link to the Web pages containing his copyrighted materials and downloaded a cached copy of those pages from Google’s system cache.¹⁹⁹⁴ As discussed in Section II.A.4(l) above, the court ruled that Google was not a direct infringer because it lacked the necessary volitional act in responding with a purely automated download process to users who clicked on the “Cached” links.

In addition, the court granted summary judgment to Google on its three defenses of implied license, estoppel, and fair use. With respect to the implied license defense, the court found that Field was aware of the industry standard mechanisms by which he could have indicated a desire not to have his Web site crawled or cached, and that, with knowledge of how Google would use the copyrighted works he placed on his site, by choosing not to include meta-tags on the site that he knew would have caused the Googlebot not to archive his site, his

¹⁹⁹⁰ Id. at 1112-13.

¹⁹⁹¹ Id. at *1113.

¹⁹⁹² Id.

¹⁹⁹³ Id. at *1113-14.

¹⁹⁹⁴ Id. at *1115.

conduct should reasonably be interpreted as a license to Google for crawling and archiving the site.¹⁹⁹⁵

The court also found that Field should be estopped from asserting a copyright claim based on the challenged behavior by Google. Field knew of Google's allegedly infringing conduct well before any supposed infringement of his works took place and knew "that Google would automatically allow access to his works through 'Cached' links when he posted them on the Internet unless he instructed otherwise."¹⁹⁹⁶ Yet, he remained silent regarding his unstated desire not to have "Cached" links provided to his Web site and intended Google to rely on this silence knowing that it would. Google was not aware that Field did not wish to have Google provide "Cached" links to his works, and Google detrimentally relied on Field's silence. Accordingly, the court found the four factors for estoppel present, and granted Google's summary judgment on the defense of estoppel.¹⁹⁹⁷

The court then turned to application of each of the four factors of the fair use defense. Concerning the first factor, purpose and character of the use, the court, relying on Kelly v. Arriba Soft,¹⁹⁹⁸ found Google's search engine was a transformative use of Field's works in that Google's presentation of "Cached" links did not serve the same functions to enrich and entertain others that Field's original posting of the works did. Rather, the "Cached" links allowed users to locate and access information that was otherwise inaccessible, and allowed users to understand why a page was responsive to their original query. The object of enabling users to more quickly find and access the information they were searching for was not served by the original page.¹⁹⁹⁹ Nor did Google's use of "Cached" links substitute for a visit to the original page. The court noted that Google had included at the top of each listing a prominent link to the original Web page. The "Cached" links were displayed in smaller font and in a less conspicuous location, and there was no evidence that Internet users accessed the pages containing Field's works via Google's "Cached" links in lieu of visiting those pages directly. Google's status as a commercial enterprise also did not negate the first factor weighing in Google's favor, because there was no evidence that Google profited in any way by the use of any of Field's works. Field's works were merely among billions of works in Google's database, and when a user accessed a page via Google's "Cached" links, Google did not display advertising to the user or otherwise offer a commercial transaction.²⁰⁰⁰

The court found that the second factor, the nature of the copyrighted works, weighed only slightly in Field's favor. Even assuming that Field's copyrighted works were creative, the court noted that he had published them on the Internet, thereby making them available to the

¹⁹⁹⁵ Id. at *1115-16.

¹⁹⁹⁶ Id. at 1116-17.

¹⁹⁹⁷ Id. at 1117.

¹⁹⁹⁸ 336 F.3d 811 (9th Cir. 2003).

¹⁹⁹⁹ Field v. Google, 412 F. Supp. 2d at 1118-19.

²⁰⁰⁰ Id. at 1119.

world at his Web site, thus indicating a desire to make his works available to the widest possible audience for free.²⁰⁰¹ The court found the third factor, the amount and substantiality of the use, to be neutral. The transformative and socially valuable purposes served by Google's caching could not be effectively accomplished by using only portions of the Web pages.²⁰⁰²

The court ruled that the fourth factor, the effect of the use upon the potential market for or value of the copyrighted work, weighed strongly in favor of a fair use determination. The court noted that here there was no evidence of any market for Field's works, and Field had made the works available to the public for free in their entirety and admitted he had never received any compensation from selling or licensing them.²⁰⁰³ In a significant holding, the court rejected Field's argument that Google's caching harmed the market for his works by depriving him of revenue he could have obtained by licensing Google the right to present "Cached" links for the pages containing his works. The court recognized the bootstrapping nature of the argument: "Under this view, the market for a copyrighted work is always harmed by the fair use of the work because it deprives the copyright holder of the revenue it could have obtained by licensing that very use. The Supreme Court has explained that the fourth fair use factor is not concerned with such syllogisms [citing *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 592 (1994)]. ... Where there is no likely market for the challenged use of the plaintiff's works, the fourth fair use factor favors the defendant."²⁰⁰⁴

Finally, the court noted that in adjudicating fair use, courts may consider other factors beyond the four enumerated ones in the copyright statute. In this case, the court found it significant that Google had acted in good faith, as evidenced by the fact that Google honored the industry standard protocols that site owners could use to instruct search engines not to provide "Cached" links for the pages of their sites. Google also provided an automated mechanism for promptly removing "Cached" links from Google's search results if undesired links ever appeared. And Google had, without being asked, promptly removed the "Cached" links to the pages of Field's site upon learning that he objected to them.²⁰⁰⁵ Accordingly, balancing all the factors, the court granted summary judgment for Google on its fair use defense.²⁰⁰⁶ As discussed further in Section II.C.5(b)(1)(ii).a below, the court also concluded that Google was entitled to the safe harbor of Section 512(b)(1) of the DMCA.²⁰⁰⁷

²⁰⁰¹ *Id.* at 1120.

²⁰⁰² *Id.* at 1120-21.

²⁰⁰³ *Id.* at 1121.

²⁰⁰⁴ *Id.* at 1121 n.9.

²⁰⁰⁵ *Id.* at 1122-23.

²⁰⁰⁶ *Id.* at 1125.

²⁰⁰⁷ *Id.* at 1123-24.

(b) Perfect 10 v. Google (aka Perfect 10 v. Amazon)

In Perfect 10 v. Google,²⁰⁰⁸ discussed in detail in Section II.C.4 above, the district court ruled, contrary to the Intellectual Reserve case discussed in Section III.D.6 above, that the caching that occurs in an Internet user's web browser constitutes a fair use:

[Plaintiff] argues that merely by viewing such websites [containing infringing photographs], individual users of Google search make local "cache" copies of its photos and thereby directly infringe through reproduction. The Court rejects this argument. Local browser caching basically consists of a viewer's computer storing automatically the most recently viewed content of the websites the viewer has visited. It is an automatic process of which most users are unaware, and its use likely is "fair" under 17 U.S.C. § 107. *But cf. Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.*, 75 F. Supp. 2d 1290 (D. Utah 1999). Local caching by the browsers of individual users is noncommercial, transformative, and no more than necessary to achieve the objectives of decreasing network latency and minimizing unnecessary bandwidth usage (essential to the internet). It has a minimal impact on the potential market for the original work, especially given that most users would not be able to find their own local browser cache, let alone locate a specific cached copy of a particular image. That local browser caching is fair use is supported by a recent decision holding that Google's own cache constitutes fair use. *Field v. Google, Inc.*, [412 F. Supp. 2d 1106 (D. Nev. 2006).] If anything, the argument that local browser caching is fair use is even stronger. Whereas Google is a commercial entity, individual users are typically noncommercial. Whereas Google arranges to maintain its own cache, individual users typically are not aware that their browsers automatically cache viewed content. Whereas Google's cache is open to the world, an individual's local browser cache is accessible on that computer alone.²⁰⁰⁹

On appeal, the Ninth Circuit affirmed this ruling, holding that, "even assuming such automatic copying could constitute direct infringement, it is a fair use in this context. The copyright function performed automatically by a user's computer to assist in accessing the Internet is a transformative use. Moreover, as noted by the district court, a cache copies no more than is necessary to assist the user in Internet use. It is designed to enhance an individual's computer use, not to supersede the copyright holders' exploitation of their works. Such automatic background copying has no more than a minimal effect on Perfect 10's rights, but a considerable public benefit."²⁰¹⁰

²⁰⁰⁸ 416 F. Supp. 2d 828 (C.D. Cal. 2006), aff'd sub nom. Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1169 (9th Cir. 2007).

²⁰⁰⁹ Id. at 852 n.17.

²⁰¹⁰ Perfect 10 v. Amazon.com, Inc., 508 F.3d 1146, 1169 (9th Cir. 2007).

(c) Ticketmaster L.L.C. v. RMG Technologies, Inc.

In Ticketmaster L.L.C. v. RMG Technologies, Inc.²⁰¹¹ the plaintiff Ticketmaster sought to hold the defendant liable for direct and indirect copyright liability based upon the defendant's development and marketing of an automated tool that enabled users (such as ticket brokers) to access and navigate rapidly through the Ticketmaster site and purchase large quantities of tickets. The court granted a preliminary injunction against the defendant, finding that the defendant was highly likely to be found liable for direct copyright infringement because it had, during the course of development of the tool, accessed the defendant's site and made copies of web pages from the site in the RAM of its computers, which copies the court held, citing MAI v. Peak, fell within the Copyright Act's definition of "copy." The court found such copying unauthorized because it violated the Terms of Use posted on Ticketmaster's site, which prohibited use of any areas of the site for commercial purposes and use of any automated devices to search the site.²⁰¹²

The court rejected the defendant's argument, based on Perfect 10 v. Google, that such RAM copying should be deemed a fair use. The court distinguished that case on the ground that the Ninth Circuit had ruled only that automatic cache copies made by users who link to infringing web sites should be deemed a fair use because, in that particular context, the caching was noncommercial, transformative and had a minimal impact on the potential market for the original work. By contrast, in the instant case, the court ruled that the defendant was not an "innocent" third party visitor to another person's infringing site. Instead, the purpose of the defendant's viewing the Ticketmaster web site and the copying that entailed was to engage in conduct that violated the site's Terms of Use in furtherance of the defendant's own commercial objectives.²⁰¹³ "Furthermore, in this case, such copying has a significant, as opposed to minimal, effect on Plaintiff's rights because Defendant's conduct empowers its clients to also violate the Terms of Use, infringe on Plaintiff's rights, and collectively cause Plaintiff" harm.²⁰¹⁴

The court also found the defendant highly likely to be liable for contributory infringement because it had supplied a tool that enabled its users to gain unauthorized access and use of the Ticketmaster site, thereby making infringing copies of web pages from the site, and had also induced the infringing behavior by advertising its tool as "stealth technology [that] lets you hide your IP address, so you never get blocked by Ticketmaster."²⁰¹⁵

²⁰¹¹ 507 F. Supp. 2d 1096 (C.D. Cal. 2007).

²⁰¹² Id. at 1105-09.

²⁰¹³ Id. at 1109-10.

²⁰¹⁴ Id. at 1110.

²⁰¹⁵ Id. at 1110-11 (emphasis in original).

(d) *Parker v. Yahoo!, Inc.*

In *Parker v. Yahoo!, Inc.*,²⁰¹⁶ the plaintiff, author of several works that he made freely available on his web site, sued Yahoo and Microsoft for copyright infringement, alleging that their search engines created and republished unauthorized cached copies of his works based on the fact that when an Internet user used either of the defendants' search engines, the search results included hyperlinks to cached copies of the web pages responsive to the user's inquiry. The user could view those search results either by following a hyperlink to the original web site or by viewing the cached copy hosted on the defendants' computers. The plaintiff conceded in his complaint that the defendants each provided opt-out mechanisms, through the robots.txt protocol, that would prevent his web sites from being cached, but that he had not made use of them.²⁰¹⁷

The court ruled that, as a result of the plaintiff's failure to employ the robots.txt protocol on his web site or to send the defendants a takedown notice, the defendants had an affirmative defense of implied license for acts of caching prior to the lawsuit. From the plaintiff's silence and lack of earlier objection, the defendants could properly infer that the plaintiff knew of and encouraged the search engines' activity. However, the court refused to dismiss entirely the plaintiff's count for direct copyright infringement because the defendants had allegedly continued to display the plaintiff's works even after the filing of the lawsuit. The court noted several decisions holding that a nonexclusive implied license can be revoked where no consideration has been given for it, and initiation of a lawsuit itself may constitute revocation of an implied license if there was no consideration for the license.²⁰¹⁸

However, the court dismissed the plaintiff's counts for contributory and vicarious copyright infringement on the part of the defendants based on allegedly infringing copies of the plaintiff's content made when an Internet user's browser stored a temporary copy of a file that was necessary for the user to view the web site. The court ruled that, by publishing his works online with no registration requirement or any other access measure taken, the plaintiff had impliedly authorized Internet users at large to view his content and, consequently, to make incidental copies necessary to view that content over the Internet. And even if search engine users did directly infringe the plaintiff's copyright, the court held that the plaintiff had not set forth any plausible allegation that either defendant financially benefitted from such infringement. Nor had the plaintiff alleged that either defendant had knowledge of any third party's infringement.²⁰¹⁹

²⁰¹⁶ 2008 U.S. Dist. LEXIS 74512 (E.D. Pa. Sept. 26, 2008).

²⁰¹⁷ *Id.* at *1-2.

²⁰¹⁸ *Id.* at *14-16.

²⁰¹⁹ *Id.* at *18-20.

5. Other Caching Cases

(a) Facebook v. Power Ventures

In Facebook, Inc. v. Power Ventures, Inc.,²⁰²⁰ the defendants operated an Internet service called Power.com that collected user information from Facebook's web site outside of the "Facebook Connect" application programmer's interface (API). After a user provided his or her user names and passwords, the Power.com service used the access information to scrape user data from those accounts. Facebook alleged that the defendants committed direct and indirect copyright infringement when they made cached copies of Facebook's web site during the process of extracting user information. The defendants brought a motion to dismiss the copyright claims. The court denied the motion, ruling that Facebook's allegation that the defendants made an unauthorized cache copy of the web site on each occasion of access to scrape data was sufficient to survive a motion to dismiss.²⁰²¹

C. Liability of Online Service Providers

Much of the Internet copyright debate has centered around the issue of copyright liability of OSPs, BBS operators, system operators, and other service providers for infringing activities taking place through their facilities. Indeed, to date, almost all of the reported Internet copyright decisions have centered around the issue of liability of OSPs and BBS operators. Copyright owners have sought to hold OSPs and BBS operators liable on theories of direct liability, contributory liability, and vicarious liability. This Section discusses each of these three theories in turn and the cases raising those theories that have been decided to date involving the Internet. This Section also discusses the relevant provisions of the DMCA that limit the liability of OSPs for the infringing acts of third parties committed through their online services.

1. Direct Liability

As discussed in detail in Section II.A.4 above, a majority of the cases decided to date require that there be some kind of a direct volitional act in order to establish direct infringement liability on the part of an OSP or BBS for infringing postings and unauthorized uses by users. For example, the Netcom court refused to hold an OSP directly liable for automatic pass through of allegedly infringing messages posted to Usenet by a subscriber.²⁰²² The subsequent MAPHIA case²⁰²³ and the Sabella case²⁰²⁴ extended the logic of Netcom, refusing to hold liable as a direct infringer the operator of a BBS for the uploading and downloading by subscribers of unauthorized copies of Sega's videogames through the BBS, even though the operator encouraged the initial uploading, because the operator had not participated in the very acts of

²⁰²⁰ 2009 U.S. Dist. LEXIS 42367 (N.D. Cal. May 11, 2009).

²⁰²¹ Id. at *1-11.

²⁰²² Religious Technology Center v. Netcom On-Line Communications Servs., 907 F. Supp. 1361 (N.D. Cal. 1995).

²⁰²³ Sega Enterprises Ltd. v. MAPHIA, 948 F. Supp. 923 (N.D. Cal. 1996).

²⁰²⁴ Sega Enterprises Ltd. v. Sabella, 1997 Copyr. Law. Dec. ¶ 27,648 (N.D. Cal. Dec. 18, 1996).

uploading or downloading themselves. And the CoStar,²⁰²⁵ Ellison,²⁰²⁶ and Perfect 10 v. Cybernet Ventures²⁰²⁷ cases suggest that an OSP will not have direct liability for infringing material posted on its service by users or available through its service on third party sites where the OSP has not encouraged such posting or had advance knowledge of it.

The logic of the Ninth Circuit's decision in Subafilms, Ltd. v. MGM-Pathe Communications Co.²⁰²⁸ also suggests there should not be direct liability for persons who merely place material on a network for subsequent unauthorized copying, display, performance or the like. Subafilms held that no independent "right of authorization" was created by the copyright statute's reference in Section 106 of the exclusive right "to do or to authorize" the acts enumerated therein. Rather, the reference to "authorize" was meant only to establish potential liability for contributory infringement on the part of a person who causes an infringement by authorizing it. Under the reasoning of the Subafilms decision, even if loading material onto a server encourages (or authorizes) copying through downloading, that authorization does not suffice for direct liability.²⁰²⁹

However, as discussed in greater detail in Sections II.A.4, II.C, and II.D above, the Frena, Webbworld, Sanfilippo and Hardenburgh cases seem to go further in their willingness to impose direct liability on a BBS operator, at least where an actor such as a BBS operator or website operator has some form of direct involvement in the anticipated acts that lead to infringement or in the infringing acts themselves (such as resale of the infringing material). Such acts of direct involvement in the infringement process may be sufficient for a finding of enough volitional activity to impose direct liability. As noted below, however, legislation limiting the liability of OSPs might negate or limit the holdings of these cases.

(a) Louis Vuitton v. Akanoc Solutions

In Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.,²⁰³⁰ the defendants operated hosting services for a number of web sites overseas from which counterfeit Louis Vuitton merchandise could be purchased. The plaintiff brought claims for direct and contributory infringement of its copyrights. A jury found the defendants liable for willful contributory infringement and awarded statutory damages, and found that the defendants were not entitled to the safe harbors of the DMCA. After the verdict, the defendants filed a motion for JMOL with

²⁰²⁵ CoStar v. Loopnet, 164 F. Supp. 2d 688 (D. Md. 2001), aff'd, 373 F.3d 544 (4th Cir. 2004).

²⁰²⁶ Ellison v. Robertson, 189 F. Supp. 2d 1051 (C.D. Cal. 2002), aff'd in part and rev'd in part, 357 F.3d 1072 (9th Cir. 2004).

²⁰²⁷ Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

²⁰²⁸ 24 F.3d 1088 (9th Cir. 1994).

²⁰²⁹ R. Nimmer, Information Law ¶ 4.10, at 4-39 (2001).

²⁰³⁰ 2010 U.S. Dist. LEXIS 85266 (N.D. Cal. Mar. 19, 2010), aff'd in part & rev'd in part on other grounds, 658 F.3d 936 (9th Cir. 2011).

respect to the claims.²⁰³¹ The defendants argued that they could not be liable for contributory copyright infringement because, among other things, the acts of direct infringement – the reproduction of counterfeit merchandise and the storage of digital images of that merchandise on the servers of their web site – occurred extraterritorially in China and the digital images could not be “copies” of the copyrighted merchandise.²⁰³²

The court rejected these arguments. With respect to territoriality, the court noted that unauthorized copying and public display of a copyrighted work within the United States triggers application of U.S. copyright law, and under Section 602, unauthorized importation into the United States of copies acquired extraterritorially is prohibited, acts which the defendants clearly had done.²⁰³³ Concerning the public display right, the court noted that the Ninth Circuit had adopted in Perfect 10 v. Amazon.com²⁰³⁴ the “server test,” under which a computer owner storing an electronic image as electronic information and serving that information directly to the user is displaying the information in violation of the copyright holder’s exclusive display right. Here, the evidence established that the defendants’ servers in China stored and served data, including pictures of the plaintiff’s copyrighted merchandise, for sale to U.S. customers, which was sufficient for direct infringement of the display right. The court also rejected the defendants’ argument that the images could not be “copies” of the physical copyrighted merchandise. Accordingly, the court denied the defendants’ motion for JMOL as to direct infringement.²⁰³⁵

(b) Flava Works v. Gunter

In Flava Works, Inc. v. Gunter,²⁰³⁶ the defendants were the operators of a web site called myVidster.com, a social networking web site through which site members could store and bookmark video files and post links to third party web sites on which the files were available. Such files were then available for other myVidster users to view or download. The plaintiff, owner of copyrights in adult entertainment products, alleged that users of myVidster had uploaded the plaintiff’s copyrighted videos and images, or links to those videos, to the site. The plaintiff sent myVidster seven DMCA notices of copyright infringing specifying the infringing material, identifying users that the plaintiff suspected to be repeat infringers, and demanding that the material be taken down. The plaintiff’s complaint did not allege that myVidster had failed to remove the material identified in the notices from the site, but did allege that after the notices were sent, the web site continued to be updated with more and more infringing material from its users. The complaint also alleged that the site did not have in place any filters or identifiers to prevent the plaintiff’s copyrighted material from being re-posted by repeat

²⁰³¹ Id. at *1-2.

²⁰³² Id. at *5-6.

²⁰³³ Id. at *7-9.

²⁰³⁴ 508 F.3d 1146 (9th Cir. 2007).

²⁰³⁵ Akanoc, 2010 U.S. Dist. LEXIS 85266 at *11-15.

²⁰³⁶ 2011 U.S. Dist. LEXIS 50067 (N.D. Ill. May 20, 2011), rev’d on other grounds, 689 F.3d 754 (7th Cir. 2012).

infringers and the site took no action to stop, reprimand or ban repeat infringers. The plaintiff sought to hold myVidster directly, contributorily, and vicariously liable for infringement of its copyrights. The defendants filed a motion to dismiss on the common law claims, although the motion was apparently not based on any of the DMCA safe harbors.²⁰³⁷

The court granted the motion with respect to the claim of direct infringement, citing the CoStar case for the proposition that to establish liability for direct copyright infringement, a plaintiff must demonstrate that the defendant engaged in volitional conduct that causes a copy to be made. Because the only volitional copying alleged in the complaint was alleged to have been done by myVidster users, not its operators, the complaint failed to state a claim for direct copyright infringement.²⁰³⁸ The court's rulings with respect to contributory, vicarious, and inducement liability are set forth in Sections III.C.2(m), III.C.3(o), and III.C.4(e) below, respectively.

On appeal, although the Seventh Circuit vacated the district court's preliminary injunction based on the other claims, the court agreed that the users who uploaded infringing copies of the plaintiff's videos, and not myVidster, were the direct infringers.²⁰³⁹

(c) Capitol Records v. Escape Media

The defendant Escape Media operated an Internet-based music streaming service called "Grooveshark." Users of Grooveshark, after accepting Escape's Terms of Service, could create free accounts and submit digital MP3 files to be uploaded to a central library of sound recordings maintained on Escape's servers. Grooveshark's library could be searched and displayed to users primarily using three metadata fields – artist, album and song. Anyone could access www.grooveshark.com, search its library for particular songs, and stream music without registering an account or providing personal information. Escape streamed files to users by storing a single master copy of each file in its central library and allowing multiple users to share access to that same file. Before an MP3 was uploaded to Grooveshark, it was run through Escape's content filtering system, which could block certain files based on their prohibited content or because the user submitting the file had had his or her uploading privileges revoked. The account holder was required to click a box before submitting files to verify that he or she understood the Terms of Service and was uploading only content that did not infringe upon the rights of others. Escape controlled what content was housed in the Grooveshark library and could block files based on their metadata or their audio fingerprints.²⁰⁴⁰

Using a "fuzzy matching" technology applied without users' participation, Escape changed the file metadata entered by users in order to group together content with similar but

²⁰³⁷ Id. at *1-4.

²⁰³⁸ Id. at *6-8.

²⁰³⁹ Flava Works, Inc. v. Gunter, 689 F.3d 754, 758 (7th Cir. 2012).

²⁰⁴⁰ Capitol Records, LLC v. Escape Media Group, Inc., 2014 U.S. Dist. LEXIS 183098 at * 42-45 (S.D.N.Y. May 28, 2014) (Report and Recommendation of magistrate judge).

not identical names and multiple files that appeared to contain the same sound recording. To further organize the content submitted by users, Escape downloaded to its servers and synced its audio library to a third-party database of commercial music content metadata called “MusicBrainz.” If metadata associated with Grooveshark content was found to be similar enough to listings in MusicBrainz, the MusicBrainz data replaced the data in the Grooveshark library. Escape also maintained metadata filters that allowed it to block content based on artist, album and song names, and to exclude duplicative content.²⁰⁴¹

With respect to user-submitted content alleged by a copyright owner to be infringing, Escape implemented what it called its “one strike policy,” under which Escape purported to disable the uploading capabilities of a user after receiving one DMCA notice asserting that the user uploaded infringing content, in addition to removing the file and sending an email notification to the user. Although Escape had no policy to identify repeat infringers, it took the position that its one strike policy precluded the possibility of repeat infringers. When Escape received a takedown request that it considered to be non-compliant with the DMCA notification requirements or ambiguous or unofficial, Escape applied a policy it created called “DMCA Lite,” under which the file was removed but the user who submitted the file did not lose uploading privileges, did not receive a notification email, and was not recorded. An Escape database titled “Takedown Batches” showed that, since the earliest entry on Feb. 13, 2013, 94.2% of the takedowns had been recorded in the “dmca_lite” field, as opposed to the “dmca” field.²⁰⁴²

Escape had no procedure for terminating a user’s account in connection with a DMCA takedown and had never terminated a user’s account for infringement. Escape had no procedure for terminating, limiting, or restricting any functionality in a user’s account beyond disabling uploading privileges, regardless of how many DMCA takedown notices the user received. Additionally, it had never removed from Grooveshark.com all content or data associated with an infringing user’s account under a repeat infringer policy, nor did it have a procedure for removing from its library all content submitted by a user who had received repeated notices of infringement. After identifying an infringing user, Escape had no policy to, and had never attempted to, block that infringing user from creating a new Grooveshark user account. Nor did it keep an independent record of when users received multiple DMCA takedown notices. When processing a DMCA takedown for an MP3 file, Escape made a record of the infringement only for the first user to submit the file; it did not make a record for any users who submitted the infringing file afterward.²⁰⁴³

In response to the plaintiff’s motion for summary judgment, a magistrate judge recommended that summary judgment be granted to the plaintiff on its claims for direct infringement of the right of performance and for both contributory and vicarious infringement.

²⁰⁴¹ Id. at *45-46.

²⁰⁴² Id. at *47-48.

²⁰⁴³ Id. at *48-50.

The magistrate recommended that the plaintiff's motion be denied with respect to its claim for direct infringement of its right of reproduction.²⁰⁴⁴

With respect to the plaintiff's claim for direct infringement of the public performance right, the court noted, citing the Second Circuit's Cablevision and Aereo cases, that generally a transmission is not public where a unique copy of a recording is created for each listener who wishes to play the recording and making each transmission is available only to the single subscriber for whom that unique copy was made. Files streamed over the Internet are typically public under this definition, and the Second Circuit had therefore found Internet streaming to produce public performances. By streaming a song on Grooveshark.com, a user was able to listen to the song only contemporaneously with the stream; a user could not receive delivery of the file of the recording. The magistrate concluded that such stream constituted a performance under the copyright act, and that performance was public because Grooveshark streamed content to users by storing a single master copy of each recording in its central library and allowing multiple users to share access to that same file. Because Grooveshark had streamed the plaintiff's copyrighted recordings without authorization millions of times, the magistrate recommended that the plaintiff be granted summary judgment on its claim for direct infringement of its right of public performance.²⁰⁴⁵

With respect to its claim for direct infringement of its reproduction right, the plaintiff argued that because Escape had discretion over whether user-submitted content was uploaded to Grooveshark and made the decision whether to copy, it should be held directly responsible for the copy that occurred during uploads. The magistrate rejected this argument, noting that there was no factual support for EMI's assertion that Escape itself made any copies during the upload process. Nor was there any submitted evidence that would allow the court to reach any conclusions as to whether the process by which Grooveshark streamed MP3 files resulted in unauthorized reproduction – i.e., evidence bearing on whether the streaming process created copies of the copyright work that were of sufficient duration or complete enough for the copy to be considered fixed under Cablevision. The magistrate therefore recommended that the plaintiff's request for summary judgment of direct infringement of its reproduction right be denied.²⁰⁴⁶

The magistrate then turned to the plaintiff's claims for secondary liability, noting first that there was a sufficient predicate of direct liability on the part of Grooveshark users – by making unauthorized copies and publicly sharing them through Grooveshark.com, Grooveshark users directly infringed the plaintiff's rights of reproduction and distribution. Turning to the plaintiff's claim for vicarious liability, the court first noted that the ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise infringing activity. Here, the undisputed evidence established that Escape had the right and ability to supervise Grooveshark users' infringing conduct, but did not exercise that

²⁰⁴⁴ Id. at *2-3.

²⁰⁴⁵ Id. at *67-68.

²⁰⁴⁶ Id. at *69-73.

right to stop infringement. Escape reserved the express right to control users' activity on Grooveshark. Users committed infringement by submitting files to be uploaded, which users could do only by registering a Grooveshark account. To register an account, users were required to agree to Escape's Terms of Service, which permitted Escape to terminate accounts, revoke privileges, and remove user-submitted content at its discretion. Escape was able to filter user-submitted content and currently did so for works owned by one small label with which Escape had an agreement. Escape could deny access by either terminating a user's account or disabling a user's uploading capability. It was able to supervise and regulate users by processing their file submissions through different filters and databases, which it currently did for purposes other than to curtail infringement.²⁰⁴⁷

With respect to the financial benefit prong, the court noted that evidence of financial gain is not necessary to prove vicarious liability as long as the service provider has an economic incentive to tolerate infringing conduct. Here, infringing content was a substantial draw to Grooveshark.com, as demonstrated by the fact that approximately 84.5% of the site's streams were of works belonging to major labels with whom Escape had no license. Approximately 80% of Escape's revenue was derived from website advertisements, and the more visitors Grooveshark attracted, the more advertising revenue it would earn. Escape thus had a clear economic incentive to tolerate the infringing users who supplied Grooveshark with its music content, as demonstrated by its promotional materials, which emphasized its large number of visitors and its music library, promoted as "the largest of any streaming service." The court therefore recommended that the plaintiff's motion for summary judgment on its vicarious liability claim be granted.²⁰⁴⁸

Turning next to the plaintiff's claim for contributory infringement, the magistrate noted that to show "material contribution," a plaintiff must establish that the defendant had actual or constructive knowledge of the infringing activity and encouraged or assisted others' infringement, or provided machinery or goods that facilitated infringement. Here, the evidence demonstrated that Escape had knowledge of the infringing activity, as shown by its own projections as to its streaming of unlicensed content and the DMCA takedown notices of infringement it received. One of its witnesses had acknowledged that the great majority of content on Grooveshark at one point came from illegal networks. In addition, the evidence established that Escape materially contributed to its users' infringement by providing the site and facilities or the environment for the infringing activity. It provided all the mechanisms to allow for infringing activity, including the servers to host and the software to submit the infringing content, the tools for organizing the submitted files and facilitating their access and search, and the interface for users to select and stream infringing content to users' devices. The court therefore recommended that EMI's motion for summary judgment on its claim for contributory infringement should be granted.²⁰⁴⁹

²⁰⁴⁷ Id. at *75-76.

²⁰⁴⁸ Id. at *77-78.

²⁰⁴⁹ Id. at *78-79.

The district court found no clear error with the magistrate’s copyright recommendations and therefore adopted them in full for the reasons given by the magistrate.²⁰⁵⁰ The district court’s rulings with respect to the DMCA safe harbor asserted by Escape are discussed in Section III.C.6(b)(1)(iii).ee below.

(d) UMG Recording v. Escape Media

In UMG Recording, Inc. v. Escape Media Group, Inc.,²⁰⁵¹ several record labels brought direct and secondary infringement claims against Escape Media and its two founders for the operation of an online music service known as “Grooveshark.” The plaintiffs sought summary judgment based solely on the direct upload of the plaintiffs’ copyrighted music by Escape Media’s employees and officers. The plaintiffs alleged that Grooveshark initially launched as a peer-to-peer sharing service. Escape Media was aware that its business model depended on the use of infringing content, but decided to launch its service utilizing infringing content in order to grow faster and attempt to strike more favorable licensing deals with the plaintiffs later. Because Grooveshark would not initially have a large user base to leverage as a source for content, Escape Media directed its employees to obtain and make available the content necessary to launch Grooveshark. Specifically, Escape Media instructed its employees and officers to create Grooveshark user accounts and to store hundreds of thousands of digital music files on their computers in order to upload or “seed” copies of those files to other Grooveshark peer-to-peer users.²⁰⁵²

A year later, Escape Media decided to move away from a peer-to-peer model. It started to use its servers as a vast central storage library for all of the music files available on the Grooveshark peer-to-peer network. As a result, users could then access all of the music on the central library regardless of the number of users online at the time. To further enhance the content in its central library, Escape Media redesigned its peer-to-peer client so that it would automatically copy every unique music file from each of its users’ computers and upload them to the central library. Less than a year later, Escape Media re-launched Grooveshark as a new streaming service that provided users with instant access to all of the songs stored in the central library without requiring users to create an account or download any software. Within a few months, Escape Media discontinued its peer-to-peer network.²⁰⁵³

Soon after the launch of the central library streaming service, Escape Media began receiving numerous DMCA takedown notices from copyright holders. Because the takedown notices threatened to diminish the Grooveshark music library, Escape’s officers searched for infringing songs that had been removed in response to DMCA takedown notices and re-uploaded infringing copies of those songs to Grooveshark. In addition, Escape Media employees regularly

²⁰⁵⁰ Capitol Records, LLC v. Escape Media Group, Inc., 2015 U.S. Dist. LEXIS 38007 at *7-11 (S.D.N.Y. Mar. 25, 2015).

²⁰⁵¹ 2014 U.S. Dist. LEXIS 137491 (S.D.N.Y. Sept. 29, 2014).

²⁰⁵² Id. at *2-7.

²⁰⁵³ Id. at *12-14.

uploaded files to Grooveshark in order to “test” the functionality of the uploading process, and all files uploaded as part of the “tests” remained in the central library. Escape Media’s internal database records of the activities of its users, including the uploading and streaming of files, confirmed the uploading of more than 150,000 files to Grooveshark by its employees, including thousands of copies of sound recordings owned by the plaintiffs. Internal records further established that Escape Media streamed copies of the infringing employee uploads millions of times to Grooveshark users.²⁰⁵⁴

The court granted the plaintiffs’ motion for summary judgment of liability on the part of Escape Media and its two founders for direct, vicarious, contributory and inducement of infringement based solely on the uploading of infringing files by its employees and management to the central library – the plaintiffs did not seek to hold the defendants liable for infringement by users of the Grooveshark service. With respect to direct infringement, the court found that the plaintiffs had established, through analysis of file metadata and use of Audible Magic’s audio fingerprinting technology to confirm that copies of certain files uploaded by the defendants corresponded to the plaintiffs’ sound recordings, that the defendants illegally uploaded 4,053 of the plaintiffs’ copyrighted sound recordings. The court also found that the plaintiffs were entitled to a finding of 1,944 additional illegal uploads based upon the defendants’ spoliation of evidence of upload activity. The court further found that Escape Media’s database records confirmed that it had streamed, or publicly performed, copies of the plaintiffs’ copyrighted sound recordings at least 36 million times. Based on this evidence, the court found that the defendants, by instructing their employees to repeatedly upload substantial volumes of popular copyrighted music files to Grooveshark, had engaged in the required volitional conduct necessary to support a finding of direct infringement.²⁰⁵⁵

The court found the defendants liable for vicarious liability because Escape Media had the right and ability to supervise and control its employees’ infringing activity, and in fact had directed its employees to engage in copyright infringement. Escape Media had received a financial benefit from the infringing employee uploads because they served as a draw for Grooveshark users. Escape Media had relied on the uploaded sound recordings to build a comprehensive music catalog in order to attract users to the service and then monetize the illegal content by generating advertising revenue and other fees.²⁰⁵⁶

The defendants were liable for inducement of infringement because Escape Media and its executives directed their employees to engage in the uploading of digital music files to Grooveshark, including overtly instructing the uploading of as many files as possible as a condition of employment. The defendants had therefore engaged in purposeful conduct with a manifest intent to foster copyright infringement via the Grooveshark service. Finally, the defendants were liable for contributory infringement because they had actual knowledge that their employees were uploading copyrighted files onto Grooveshark, and they materially

²⁰⁵⁴ Id. at *14-17.

²⁰⁵⁵ Id. at *19, *54-56 & *70.

²⁰⁵⁶ Id. at *63-64.

contributed to the infringing conduct by actively instructing employees to upload copyrighted sound recordings. Additionally, senior Escape Media officers had personally participated in the infringing activity and made their home Internet connections available to increase the number of uploaded files.²⁰⁵⁷

In April of 2015, as part of a settlement with the plaintiffs, Grooveshark agreed to shut down, thereby avoiding a looming jury verdict that could have left the company owing \$736 million in statutory damages, and issued a lengthy apology to the music industry. The settlement also required the company to wipe clean all the data on its servers and hand over ownership of its website, its mobile apps and intellectual property, including its patents and copyrights. The tech blog Re/Code reported that the deal would require no payment from Grooveshark other than a \$75 million fine in the event of a breach of the agreement.²⁰⁵⁸

(e) Milo & Gabby v. Amazon.com

The court's rulings with respect to direct liability in this case are discussed in Section III.C.6(b)(1)(iii).gg below.

(f) Smith v. Barnesandnoble.com

In this case, the plaintiff Smith owned the copyright in a book that he authorized an eBook distributor, Smashwords, Inc., to make available for sale and sampling both on Smashwords' own web site and on the web sites of its retail partners. Pursuant to the agreement, Smashwords furnished the book to the defendant Barnesandnoble.com under a partner agreement in which the defendant was entitled to distribute up to 5% of an eBook's content free as a sample. The defendant made Smith's book available to customers through its cloud-based "Digital Locker" system. Each time a customer acquired digital content from the Barnesandnoble.com site, a listing for that content was saved in the customer's personal digital locker, appearing in the library of the customer's e-reader, on a software application for accessing the site, and on the customer's account on the web site. Only a single Barnesandnoble.com customer acquired a free sample of the book from the web site, and it was saved to her digital locker. More than a year later, Smith terminated his agreement with Smashwords and notified Smashwords to de-publish his work and delete his account immediately. Because of Smith's insistence that his account be deleted immediately, a "takedown notice" that was normally automatically generated to retailers informing them of the de-publication event was also deleted. As a result, Smith's book remained listed on the defendant's web site even after Smith ended his agreement with Smashwords. Smith's lawyer sent notification to the defendant of copyright infringement and threatened legal action, and the same day the defendant removed the listing of the book from its web site. However, the defendant did not remove the free sample of the book from the digital locker of the lone

²⁰⁵⁷ *Id.* at *65-67.

²⁰⁵⁸ Bill Donahue, "Grooveshark Settles With Labels, Agrees to Shut Down," *Law360* (Apr. 30, 2015), available as of May 3, 2015 at <http://www.law360.com/articles/650463>.

customer who had downloaded it. The sample was subsequently re-downloaded to two distinct e-reader devices at two distinct IP addresses, both associated with such customer's account. Smith filed an action for direct and contributory copyright infringement against the defendant on grounds of unauthorized reproduction and distribution. The defendant moved for summary judgment.²⁰⁵⁹

The court rejected Smith's claim for direct infringement because the required volitional element was missing. The court noted that, while the defendant had a license to distribute the content at the time the content was selected by the customer, that license may have expired by the moment of the re-download requests. However, as in the Second Circuit's Cablevision case, the lack of license at that later time did not mean the defendant engaged in volitional conduct sufficient to support a copyright infringement claim. The re-downloads of Smith's work had all occurred as the result of an automated response by the defendant's Digital Locker system. Because there was no evidence that the defendant hosted unlicensed copyrighted materials in its digital lockers, this case was distinguishable from those in which defendants were found to have engaged in volitional conduct even though a user or customer pressed the button to make a copy. In those cases, unlike here, the defendants actively encouraged and benefited from the infringing copying activity and in fact set up their services around such activity. The lack of volitional conduct on the part of the defendant therefore precluded Smith's claim for direct copyright infringement under a theory of either reproduction or distribution.²⁰⁶⁰

The court also rejected Smith's claim for contributory infringement, under which Smith was required to show that the defendant knew or had reason to know of the direct infringement that occurred by virtue of the two re-downloads and made a material contribution to such infringement. The court noted as an aside that there was a question whether the customer's possibly unintentional re-downloads of a previously authorized sample constituted infringing acts at all. The court cited authority for the proposition that an individual may move copyrighted materials around on his or her personal hard drive without infringing on copyrights. The court noted that to hold the defendant's customer may not move material between her personal hard drive and her personal cloud-based digital locker without infringing would have far-reaching consequences for the many users of cloud-based storage systems like Dropbox or Apple's iCloud – particularly as it is not always clear to the user what is stored locally and what is stored in the cloud.²⁰⁶¹

However, the court concluded that it need not decide whether the customer's actions in this case constituted infringement, because, even if so, the defendant could not be held liable for contributory infringement because, under the Sony doctrine, the defendant's Digital Locker system was capable of substantial non-infringing uses, and those uses were commercially significant. That non-infringing capability set the defendant apart from defendants in other cases who provided the site and facilities for infringement and were found liable under theories

²⁰⁵⁹ Smith v. Barnesandnoble.com, LLC, 143 F. Supp. 3d 115, 11819 (S.D.N.Y. 2015).

²⁰⁶⁰ Id. at 121-23.

²⁰⁶¹ Id. at 124-25.

of contributory infringement.²⁰⁶² The court observed that “noninfringing use must be near-impossible for summary judgment in favor of plaintiffs to be appropriate on this sort of claim.”²⁰⁶³ Accordingly, the court granted the defendant summary judgment on Smith’s claims for both direct and contributory infringement.²⁰⁶⁴

On appeal, the Second Circuit affirmed, but on contractual grounds without reaching the copyright issues. The court noted that the agreement between the parties provided for the distribution of samples with a license for free, noncommercial use, duplication and sharing, without any provision to terminate the license for samples already distributed in the event the distribution agreement itself was terminated. The agreement contemplated robust sampling rights, and Smashwords prohibited authors from using digital rights management schemes that would limit a customer’s ability to consume the authors’ work as they saw fit. The court noted the plaintiff did not argue that a customer who purchased the book itself would lose cloud-based access to it upon termination of a distribution agreement, and the license granted in the agreement to access the free sample was no more restrictive or limited than the license to access the book itself after purchase. Once the customer acquired the cloud-based sample, the service that the defendant provided was no longer distribution, but rather access. Accordingly, the Second Circuit concluded that the district court was correct to grant the defendant’s motion for summary judgment, and therefore affirmed that judgment, albeit on different grounds.²⁰⁶⁵

(g) BWP Media v. Polyvore

The plaintiff was the owner of copyright in photographs that appeared without authorization on the defendant’s Polyvore web site, which hosted a user-curated community that allowed users to create and share digital collages devoted to fashion, art and design. The defendant offered an online tool called the Clipper that allowed users to clip images from other web pages and collect those images on Polyvore’s platform. Once uploaded by a Polyvore user, each image received a hyperlink that linked back to the original site the image came from and a unique URL that identified the precise location of the image on Polyvore’s web site. All images displayed on Polyvore, whether in a personalized collage created by a user or as a search result, were displayed automatically by software and without any interaction by the defendant’s employees. The defendant did not screen the source sites or content before displaying images on its web site. The defendant brought claims for direct, contributory, vicarious and inducement liability.²⁰⁶⁶

²⁰⁶² Id. at 125-26.

²⁰⁶³ Id. at 126.

²⁰⁶⁴ Id. at 126-27.

²⁰⁶⁵ Smith v. Barnesandnoble.com, LLC, 839 F.3d 163, 167-68 (2d Cir. 2016).

²⁰⁶⁶ BWP Media USA Inc. v. Polyvore, Inc., 2016 U.S. Dist. LEXIS 92121 at *1-5 (S.D.N.Y. July 15, 2016), aff’d in part & rev’d in part, 922 F.3d 42 (9th Cir. 2019).

The court granted the defendant summary judgment on direct infringement on the basis that the plaintiff had not proved the volitional conduct requirement under the Second Circuit's Cablevision case. Citing the Smith v. BarnesandNoble.com case discussed in Section III.C.1(f) above, the court noted that, in determining whether a defendant who designs and houses an automated system acts volitionally post-Cablevision, courts have looked to the purpose and general use of the service in question, finding volitional conduct where a service or program was designed solely to collect and sell copyrighted material, and where a program collected material that its creators knew to be copyrighted. In this case, no reasonable juror could find that Polyvore acted volitionally. It was undisputed that images appeared on Polyvore's web site without an interaction by Polyvore's employees and that any subsequent indexing, storage or display was the result of an automated process that stemmed from the user's initial upload. Nothing in the record suggested that Polyvore's Clipper tool was designed specifically to infringe anyone's copyright interests, and it allowed users to clip images from anywhere online, not just locations that displayed only copyrighted images.²⁰⁶⁷

The court rejected the plaintiffs' arguments that Cablevision's volitional conduct requirement should not apply in this case because Polyvore, unlike the defendants in Cablevision, was a service provider that could invoke the safe harbor provisions of the DMCA. The plaintiffs argued that implicit in Section 512 and the purposes of the DMCA was a recognition that, absent the safe harbor, a service provider would be held liable for infringements uploaded by a user. The plaintiffs argued that the volitional conduct requirement was accordingly inconsistent with the safe harbors in that service providers could avoid liability by ensuring they qualified for a safe harbor. The court rejected these arguments, noting that the text of the DMCA and its legislative history made clear that the DMCA does not excuse a plaintiff from establishing volitional conduct simply because the defendant is a service provider. The DMCA expressly provides in Section 512(l) that the failure of a service provider's conduct to qualify for the safe harbors shall not bear adversely upon the consideration of a defense by the service provider that its conduct is not infringing under copyright law or any other defense. And both the House and Senate reports recommending that the DMCA be passed clarified that Section 512 is not intended to imply that a service provider is or is not liable as an infringer either for conduct that qualifies for a safe harbor or for conduct that fails to so qualify. Accordingly, Polyvore was entitled to summary judgment on direct infringement.²⁰⁶⁸

The court also granted summary judgment on the plaintiffs' claims for secondary liability. With respect to contributory liability, even assuming that Polyvore had knowledge of the infringing activity and materially contributed to copyright infringement, the Sony rule shielded Polyvore from liability because the Clipper tool allowed users to clip images from anywhere online, copyrighted or not. Polyvore's system therefore was capable of substantial noninfringing

²⁰⁶⁷ Id. at *13-16.

²⁰⁶⁸ Id. at *17-18, 22. The court also rejected the plaintiffs' argument that, because the majority opinion in the Supreme Court's Aereo decision did not mention the volitional conduct requirement, Polyvore could be held liable for direct infringement regardless of the commission of a volitional act. Id. at *20 n.1.

use.²⁰⁶⁹ Polyvore was entitled to summary judgment with respect to vicarious liability because the record was devoid of evidence regarding Polyvore's ability to supervise or control the activity of its users and no facts in the record established a causal relationship between any infringing activity on Polyvore's web site and any financial benefit Polyvore received. Nor did any facts in the record establish that Polyvore's users were attracted to the site because it enabled infringement. Finally, Polyvore was entitled to summary judgment that it did not induce infringement because no evidence in the record supported an inference that Polyvore purposefully sought to infringe copyrights.²⁰⁷⁰

On appeal, the Second Circuit affirmed in part and reversed in part in a short per curiam opinion. All three panel judges wrote separate opinions. The substance of the per curiam opinion is the following paragraph:

We conclude that the district court's grant of summary judgment to Polyvore on the direct infringement claim was error because there is a dispute of material fact regarding whether Polyvore created multiple copies of BWP's photos that were not requested by Polyvore users. We further conclude that questions of material fact preclude us from holding at this state that Polyvore satisfied the requirements for the Digital Millennium Copyright Act (DMCA) § 512(c) safe harbor, even though BWP has not shown that Polyvore's stripping of metadata disqualifies it from safe harbor protection. We agree with the district court, however, that Polyvore is entitled to summary judgment on BWP's secondary infringement claims of contributory, vicarious, and inducement of infringement because the district court found that BWP abandoned those claims. And we find no error in the district court's decision not to sanction BWP. We therefore AFFIRM the district court's grant of summary judgment dismissing BWP's secondary infringement claims, AFFIRM the denial of attorney's fees, VACATE the judgment as to direct infringement, and REMAND for further proceedings pursuant to the principles and procedures set out [in] United States v. Jacobson, 15 F.3d 19 (2d Cir. 1994). We request that the district court file its response within 60 days from the issuance of this opinion or as soon as practicable thereafter, and that upon such determination, the parties promptly notify the clerk of this court, whereupon jurisdiction will be restored to this court.²⁰⁷¹

The court further noted that Judge Walker's separate concurring opinion specified the questions of material fact that remained for determination by the district court.²⁰⁷² Judge Newman concurred in the result with a separate opinion. Judge Pooler concurred in the result with a separate opinion.

²⁰⁶⁹ Id. at *23-24.

²⁰⁷⁰ Id. at *24-25.

²⁰⁷¹ BWP Media USA, Inc. v. Polyvore, Inc., 922 F.3d 42, 44 (2d Cir. 2019).

²⁰⁷² Id.

The disagreements in the separate opinions revolved mostly around the volitional requirement for direct infringement, including its scope and meaning and whether that requirement survived the Supreme Court’s decision in American Broadcasting Companies, Inc. v. Aereo, Inc.²⁰⁷³ Judge Walker argued that Aereo did not disturb the volitional conduct requirement and that requirement continues to apply to cases involving OSPs. But he found that the plaintiffs produced sufficient evidence of additional unrequested copying by Polyvore of the plaintiffs’ images to raise a question of material fact about whether Polyvore, separate from its users, acted volitionally by making and displaying the additional copies of the images. In his view, OSPs that provide additional unrequested copies of copyrighted material in response to a user’s request for a single copy can be liable for direct infringement. He disagreed with Judge Newman’s concurring opinion that the volitional conduct requirement should be understood as a causation requirement, and in particular a proximate causation requirement rather than “but for” causation. With respect to the Section 512(c) safe harbor, Judge Walker noted a question of material fact as to whether Polyvore’s additional copies were made solely to facilitate access by users. Polyvore, as the party with the burden to provide its affirmative defense, had not pointed to evidence that showed, assuming the copies were made, why they were made at all.²⁰⁷⁴

Judge Newman cited the Nimmer copyright treatise to argue that “volition” should best be understood to mean a concept essentially reflecting tort law causation, since courts had long held before the Netcom decision that copyright infringement is a tort. And the Nimmer treatise makes clear that causation, in the copyright infringement context, is tort law proximate cause rather than “but for” causation.²⁰⁷⁵ Judge Newman observed that many courts, including the Second Circuit, have clearly understood volition to mean causation, and the Cartoon Network case stated that “*Netcom* and its progeny direct our attention to the volitional conduct that *causes* the copy to be made.”²⁰⁷⁶ Judge Newman expounded, however, that tort law principles of causation do not necessarily apply in the copyright field exactly as they apply with respect to torts generally or joint tortfeasor liability in particular. The case law, he observed, had not yet developed clear principles for determining when the developer or operator of a system, activated automatically by a user, is jointly liable with the user for direct infringement. Although he agreed that the requirement of volitional conduct must be shown when there is dispute as to which party or parties caused a direct infringement and Aereo did not abrogate the requirement of such conduct, Judge Newman stated that he disagreed with Judge Walker’s opinion to the extent it appeared to suggest that all developers or operators of systems that make copies, at a customer’s keystroke command, of copyrighted materials selected by the customer should be

²⁰⁷³ 573 U.S. 431 (2014).

²⁰⁷⁴ Polyvore, 922 F.3d at 47-54, 58-59. In a footnote, Judge Walker observed that Judge Newman’s concurrence correctly noted that volitional conduct is not a legal component of a direct liability cause of action, and that the use of the term “element” in the Cablevision opinion was therefore somewhat imprecise. As the author of the Cablevision opinion, Judge Walker noted that he agreed that volitional conduct is not an element of a cause of action for direct liability, but rather a factual component that must be established when the identity of the infringer is in doubt. Id. at 48 n.4.

²⁰⁷⁵ Id. at 61-63.

²⁰⁷⁶ Id. at 63 (quoting Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121, 131 (2d Cir. 2008) (emphasis added)).

insulated from direct liability for infringement. He concluded, however, that there was no need to make any definitive ruling on the significance of selection by the customer at this stage of the pending litigation.²⁰⁷⁷

Judge Pooler wrote a very short opinion concurring in the result in which she stated that, regardless whether the volitional conduct requirement is properly understood as a causation requirement, the question will boil down to whether Polyvore was sufficiently tied to the act of copying for direct infringement liability to attach. She expressed strong line-drawing concerns with Judge Walker's statement that an ISP does not act volitionally when it automatically makes a single copy in response to a user's request but ISPs that provide additional unrequested copies in response to a user's request for a single copy may be liable. She found no basis to conclude that "additional unrequested copies" are of any significance when a machine is simply a passive agent. While she concurred in the result of remanding to the district court for further factfinding, she could not agree with conceptualizing volitional conduct in such a way that an ISP does not act volitionally when it automatically makes one, but not more than, unrequested copy in response to a user's request for a copy.²⁰⁷⁸ She expressed the belief that the volitional conduct analysis "must enter the landscape of multiple devices, mindful of both our copy-shop past and the realities of functional website design in our present."²⁰⁷⁹

(h) **Live Face on Web v. Biblio Holdings**

The plaintiff Live Face on Web (LFOW) was the developer of "live person" software that allowed companies to display a video of a walking and talking personal host to welcome online visitors to a web site. An LFOW customer implemented the LFOW software by embedding an HTML script tag in the HTML code of its web site. The added code linked the web site to a copy of the LFOW software. The copy could be stored on the same server as the customer's web site or on a different server. When a web browser was directed to a web page linked to the LFOW software, the embedded HTML script tag was read by the browser, resulting in a distribution of the LFOW software. The browser automatically saved the LFOW software into cache or a hard drive or both, and automatically loaded the LFOW software into RAM. As a result, the specific spokesperson video was launched and displayed on the web page.²⁰⁸⁰

LFOW alleged that the defendants had used an infringing version of the LFOW software to display a spokesperson video on the defendants' web site. The defendants included code on their web site to link it to a URL on a web server at tweople.com, which in turn linked to a file containing an allegedly infringing copy of LFOW's software. LFOW alleged that when a user's browser retrieved a web page from the defendants' web site, a copy of the infringing software was stored on the visitor's computer in cache, memory and/or its hard drive. LFOW brought

²⁰⁷⁷ Id. at 65-67.

²⁰⁷⁸ Id. at 69.

²⁰⁷⁹ Id.

²⁰⁸⁰ Live Face on Web, LLC v. Biblio Holdings LLC, 2016 U.S. Dist. LEXIS 124198 at *103 (S.D.N.Y. Sept. 13, 2016).

claims for direct, contributory and vicarious infringement of LFOW's copyright. The defendants moved to dismiss the complaint, in connection with which they submitted an affidavit stating that the defendants had in good faith paid Tweople for hosting and playing a video on the defendants' web site to welcome visitors, and that Tweople had sent the defendants marketing materials claiming exclusive rights to its video technology.²⁰⁸¹

With respect to direct infringement, the defendants argued that any infringing distribution was done by Tweople, whose server stored and disseminated the infringing file directly to the defendants' web site visitors. The district court noted that some authority might support the defendants' argument, notably the Ninth Circuit's decision in Perfect 10 v. Google,²⁰⁸² in which the Ninth Circuit rejected Perfect 10's argument that Google displayed or distributed infringing copies of Perfect 10's photos by virtue of framing inline-linked full size images of the photos. Google's search engine merely communicated HTML instructions that told a user's browser where to find the full size images on a third party web site, and the web site's computer performed the actual distribution. The district court noted that the reasoning of that case appeared to limit LFOW's ability to hold the defendants liable for direct infringement of LFOW's distribution right. Nevertheless, as this subject was hardly briefed and there had not been factual development in this case, the court ruled that it would permit discovery on the relationship between Tweople and the distribution of the allegedly infringing software.²⁰⁸³

The court rejected the defendants' argument that any storage of the infringing software on its users' systems was only for a transitory duration and therefore not sufficiently fixed so as to create a copy. The court noted that, to the extent the duration of storage on users' systems was relevant, it presented an issue of fact that precluded dismissal. The court also rejected the defendants' argument that their web site was protected under the safe harbor provisions of the DMCA because the complaint itself did not establish the facts necessary to sustain the safe harbor defense on a motion to dismiss. Accordingly, the court denied the defendants' motion to dismiss the direct infringement claim.²⁰⁸⁴

The court granted the defendants' motion to dismiss the contributory infringement claim on the ground that the complaint contained only a bare legal conclusion that the defendants intentionally induced and/or encouraged direct infringement by distributing the infringing version of the LFOW software via the web site and/or seeking out the LFOW software in order to use it on their web site. The court found that nothing else in the complaint suggested that the defendants knew or had reason to know that they were using an infringing version of the LFOW software, and LFOW did not argue otherwise in its brief.²⁰⁸⁵

²⁰⁸¹ Id. at *3-5.

²⁰⁸² 508 F.3d 1146 (9th Cir. 2007).

²⁰⁸³ Biblio, 2016 U.S. Dist. LEXIS 124198 at *9-12.

²⁰⁸⁴ Id. at *13-14.

²⁰⁸⁵ Id. at *18.

The court ruled, however that the complaint adequately stated a claim for vicarious infringement sufficient to avoid the motion to dismiss. LFOV had alleged that the defendants had the right and ability to modify their own web site or to have their web site modified on their behalf, and that they did modify the web site to include code linking to the infringing software. The defendants thus plausibly controlled the allegedly unlawful distribution of copies of the LFOV software to their web site visitors. LFOV also had alleged that the defendants profited from and had a direct financial interest in the infringement because use of the infringing software allowed them to capture, hold and prolong the attention of the average online visitor, and such use did in fact generate revenues and profits for the defendants. Accordingly, the court denied the motion to dismiss as to the vicarious infringement claim.²⁰⁸⁶

(i) VHT v. Zillow Group

The District Court Decision

This case arose from Zillow's alleged unauthorized use of 28,124 copyrighted real estate photographs of VHT in conjunction with a content area on Zillow's web site known as "Digs," which was geared toward home design and renovation. Zillow received millions of photos each day through feeds provided by real estate brokers and multiple listing services, which it characterized as "evergreen" (provided through the feed with unlimited temporal scope) and "deciduous" (subject to a requirement to cease displaying the photos after the corresponding listing was removed). Zillow also allowed users to upload their own images to Digs. Starting in 2014, Zillow allowed users to "dig" images from home details pages on Zillow's main web site. When a user would dig an evergreen image, the image would be accessible to any Digs user, but each deciduous image would be visible only to the user that dug the image. In addition, Zillow created a functionality called "implicit digs," in which Zillow saved to Digs images that it users selected to save but failed to finish saving. Zillow also tagged, and thereby made searchable, some of the evergreen images that Digs users selected. Zillow determined which images to make searchable through a moderation process. When the moderator gave an image a "great" quality rating, a Zillow design moderator reviewed the image and overlaid product bubbles on the "interesting products" in the image. A jury found that Zillow directly infringed on all 28,124 of the VHT photos on Digs. The jury also found that Zillow contributorily and vicariously infringed VHT's copyrights, but because the verdict form instructed the jury not to double-count Zillow's infringement, it was unclear how many copyrights the jury found Zillow indirectly infringed. The jury also rejected Zillow's affirmative defenses of license and fair use. Zillow sought JNOV with respect to the vast majority of the VHT photos.²⁰⁸⁷

The court turned first to the issue of direct liability. Zillow relied heavily on the Ninth Circuit's decision in Perfect 10, Inc. v. Giganews, Inc.,²⁰⁸⁸ which confirmed that direct copyright infringement has a causation component, often referred to as volitional conduct, that a plaintiff

²⁰⁸⁶ Id. at *18-21.

²⁰⁸⁷ VHT, Inc. v. Zillow Group, Inc., 2017 U.S. Dist. LEXIS 95010 at *2-3, *4-9 (W.D. Wa. June 20, 2017).

²⁰⁸⁸ 847 F.3d 657 (9th Cir. 2017).

must prove. The court ruled as a preliminary matter that, under Giganews, to support the jury's entire verdict, VHT could not merely show legally sufficient evidence that Zillow took volitional conduct toward some subset of the VHT photos, but rather it must show substantial evidence of volitional conduct as to each category of the VHT photos that Zillow challenged. The court then analyzed each of those categories.²⁰⁸⁹

The court first considered direct liability with respect to the rights of reproduction, derivative works, distribution, and display pertaining to the category of 22,109 VHT photos that were not displayed. With respect to the reproduction right, VHT argued that Zillow made the decision to create 16 Digs-specific copies of each photo added to Digs and wrote the algorithms to cause those copies to be created. The court rejected this argument, noting that the number of copies Zillow designed its systems to create was irrelevant to what entity or entities – Zillow, its users, or some combination – proximately caused the infringement of VHT's reproduction right. VHT further argued that Zillow engaged in volitional conduct when it decided to change course and allow reproduction of Digs-specific copies of deciduous images. The court ruled that evidence was insufficient to advance VHT's theory that Zillow directly infringed VHT's reproduction right. Finally, VHT pointed to the implicit digs process, contending it would be illogical to conclude that users who failed to complete their dig engaged in the volitional act that caused the implicit Dig copies to be created. The court noted that, in this context, volition does not refer to acts of willing, choosing, or deciding, but rather whether a defendant-host's actions are sufficiently proximate to the copying to displace or join the customer as the person who "makes" the copies. Although the user's interaction with an implicitly dug image was slightly different from the user's interaction with a dug image, no evidence suggested that Zillow took any action toward implicitly dug images that it did not take toward every image that a user followed through in posting to Digs. Rather, Zillow's system, including implicit digs, responded automatically to users' input without intervening conduct by Zillow. There was thus no legally relevant distinction between implicit digs and Digs's regular functionality. The court therefore concluded that a rational juror could not have found in favor of VHT for direct infringement of the reproduction right in the undisplayed VHT photos.²⁰⁹⁰

With respect to the derivative works right, VHT relied on the fact that Zillow's automated systems created one or more scaled copies of every image that users added to Digs. The court rejected this, noting that Zillow's systems functioned identically for the millions of non-infringing photos uploaded daily and the comparatively few infringing VHT photos that Zillow's users uploaded. There was therefore insufficient evidence at trial from which a reasonable juror could conclude that Zillow caused a violation of VHT's derivative works right in the undisplayed photos.²⁰⁹¹

With respect to the display right, VHT argued that Zillow violated its display right by "making available" the VHT images on Digs. The court noted the Copyright Office's position that

²⁰⁸⁹ Zillow, 2017 U.S. Dist. LEXIS at *13-15.

²⁰⁹⁰ Id. at *17-21.

²⁰⁹¹ Id. at *21-22.

United States law fully protects the making available right, that Section 106(5) confers an exclusive right to offer the public access to images on demand, and that the display right can be violated when a defendant makes an image available to the public rather than when the public accesses the image. The court observed, however, that VHT's proposed jury instruction on the display right did not include this corollary theory of liability and VHT did not take exception to the court's instruction on direct infringement of the display right. The court ruled that a legal theory, no matter how theoretically viable, cannot sustain a verdict where the plaintiff never presented the theory to the jury. For this reason alone, the jury had no rational basis on which to conclude that images they had been directed to treat as undisplayed were, in fact, displayed. But the court went on to rule that, even ignoring that VHT never presented this theory to jury and assuming the Copyright Office's expansive interpretation of the making available right is legally sound, the volitional conduct requirement precluded Zillow from being held directly liable for infringing the display right in the substantial majority of the undisplayed VHT photos. In the Internet context, a passive host whose systems merely automatically store information, and whose users select the images to be copied, stored, and transmitted, does not proximately cause copying and cannot be held directly liable for infringing the display right. Accordingly, there was insufficient evidence for a reasonable juror to find that Zillow infringed VHT's display right in the undisplayed VHT photos.²⁰⁹²

Finally, with respect to the distribution right, Zillow argued there was no evidence the VHT photos that Zillow merely stored on its servers were ever distributed, and those images cannot be deemed distributed under the "deemed distribution rule," which holds that the owner of a collection of works who makes them available to the public may be deemed to have distributed copies of the works.²⁰⁹³ VHT did not dispute the absence of direct evidence that Zillow violated its distribution right in the undisplayed VHT photos, but resisted Zillow's argument regarding the deemed distribution rule, although only in a three-sentence footnote located in the section of its brief pertaining to the display and derivative work rights. The court agreed with Zillow that it should not consider the deemed distribution rule here because VHT failed to properly disclose it during the course of litigation. The court thus concluded that VHT failed to present substantial evidence that Zillow directly infringed VHT's distribution right in the undisplayed VHT photos. The court therefore granted Zillow JNOV with respect to the direct infringement verdict as to the undisplayed VHT photos.²⁰⁹⁴

The court next turned to the direct infringement verdict with respect to 2,094 non-searchable photos out of 6,016 VHT photos that were displayed. The court noted that Zillow treated the non-searchable, displayed VHT photos differently by subjecting them to moderation. Zillow designed its systems to place evergreen, non-searchable, displayed VHT photos in a queue for potential moderation. First, an automated moderation filtered out images that were

²⁰⁹² Id. at *22-27.

²⁰⁹³ Id. at *27 & n.17 (reciting the definition of the deemed distribution rule from Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1162 (9th Cir. 2007) (citing Hotaling v. Church of Jesus Christ of Latter-Day Saints, 118 F.3d 199, 203 (4th Cir. 1997)).

²⁰⁹⁴ Zillow, 2017 U.S. Dist. LEXIS 95010 at *27-31.

particularly blurry or tilted. Any images that passed the automated moderation went to a queue for human moderation. If the human moderator found the image of sufficient quality, the moderator promoted it to the searchable set of images. Human moderators also had the discretion to remove images from Digs. The court ruled that merely subjecting the images to the potential for moderation did not constitute volitional conduct. And including user-selected images in a moderation queue did not constitute volitional conduct sufficient to transform Zillow from a passive host to a direct cause of the display of VHT's images, citing Giganews. The court therefore concluded as a matter of law that Zillow did not directly infringe the 2,094 non-searchable, displayed VHT photos through Digs.²⁰⁹⁵

Zillow next sought JNOV regarding 3,438 of the 3,921 displayed, searchable VHT photos that lacked evidence of actual display. Zillow argued the evidence showed only that the images appeared on users' boards, where visitors could view them without Zillow having influenced them to do so in any way through its moderation, indexing, and tagging process. But based on testimony from a Zillow program manager regarding the most common way users interacted with Digs and the disproportionate frequency with which users viewed searchable images, the jury could have reasonably concluded that users accessed those images through Digs's search function. To the extent users accessed the images through Digs's search function, the jury could have reasonably concluded that Zillow's moderation efforts, which rendered those images searchable, proximately caused the copying. Accordingly, the court denied Zillow's motions for JNOV as to the 3,438 displayed, searchable VHT photos.²⁰⁹⁶

The court then reviewed the jury's verdicts with respect to indirect infringement. Turning first to contributory infringement, the court summarized the rule in the Ninth Circuit that one contributorily infringes when he (1) has knowledge of another's infringement and (2) either (a) materially contributes to or (b) induces that infringement. A copyright owner can prove material contribution by showing that a computer system operator has actual knowledge that specific infringing material is available using its system and can take simple measures to prevent further damage to copyrighted works, yet continues to provide access to infringing works. VHT suggested that developing or licensing technological tools to identify and remove infringing images were simple measures available to Zillow, pointing to testimony by the development manager for the Digs software engineering team that he could create a tool capable of removing thousands of images in 16 hours. The court noted, however, that the testimony was that the 16 hours were predicated on additional work that preceded them, and that the removal tool would be ineffective unless Zillow first obtained the ability to identify VHT's images. VHT further argued that developing or licensing watermark-identifying software constituted a simple method by which Zillow could have identified the VHT photos. The court found, however, that the evidence failed to support that position. Testimony of a VHT witness established only that watermark-identifying software existed, but there was no reasonable basis

²⁰⁹⁵ Id. at *31-34.

²⁰⁹⁶ Id. at *34-35. As to the remaining 483 displayed, searchable VHT photos that were "searchable only," Zillow conceded that VHT presented sufficient evidence to uphold the jury's direct infringement verdict. Id. at *34 n.19.

to infer based on the existence of such software that it was available and simple for Zillow to use, particularly in view of the infrequency with which VHT watermarked its images. In sum, the court noted that, like in Giganews, VHT's notices to Zillow of infringement failed to uniquely identify infringing images and Zillow's only manner of identifying those images was onerous. Accordingly, VHT provided insufficient evidence for a reasonable juror to conclude that there were simple measures available that Zillow failed to take to remove VHT's works from Digs.²⁰⁹⁷

The court also concluded that the trial record contained insufficient evidence to hold Zillow liable for contributory infringement by inducement. After a review of the evidence presented at trial, the court found that none of it suggested that Zillow promoted the use of Digs specifically to infringe copyrights. Accordingly, the court granted Zillow JNOV on VHT's contributory infringement claims as to all but 131 VHT photos that were created on Digs after VHT first specifically identified the image.²⁰⁹⁸

The court then reviewed the jury's verdict with respect to vicarious infringement. The court recited the test for vicarious infringement in the Ninth Circuit as requiring proof that a defendant has (1) the right and ability to supervise the infringing conduct and (2) a direct financial interest in the infringing activity. The first element requires that the defendant have both a legal right to stop or limit the directly infringing conduct, as well as the practical ability to do so. The court acknowledged that the "simple measures" test for the material contribution element of contributory infringement differs from the "practical ability" test for the control element of vicarious infringement. However, the court concluded that the trial record lacked substantial evidence of a practical ability to limit direct infringement for the same reasons it lacked substantial evidence of simple measures to remove infringing material. As to all of the VHT photos besides those added to Digs after VHT first specifically identified them, Zillow lacked the practical ability to police its users' infringing conduct, because it could not reasonably identify which of the millions of images uploaded each day were infringing. The evidence unequivocally suggested that infringing images were the rare exception, not the norm, and that Zillow required each user to certify its scope of rights. Without the practical ability to independently identify infringing images, Zillow could not police its users, and the record therefore lacked substantial evidence of vicarious infringement as to all but 114 of the VHT photos that were created on Digs after VHT first specifically identified the image.²⁰⁹⁹

Finally, the court concluded that substantial evidence supported the jury's rejection of Zillow's fair use affirmative defense. Zillow's arguments analyzed fair use only from Zillow's perspective and pointed to no evidence of Zillow's users' purpose. Whatever Zillow's purpose,

²⁰⁹⁷ Id. at *37-41.

²⁰⁹⁸ Id. at *42-45.

²⁰⁹⁹ Id. at *45-47.

the jury could have reasonably concluded that its users were selecting images for Digs with a different purpose.²¹⁰⁰

The court denied VHT's motion to amend the judgment to permanently enjoin Zillow from directly and indirectly infringing on the VHT photos on Digs. The court found there was no showing that the defendant was likely to continue to infringe and an inadequate showing of irreparable harm.²¹⁰¹

The Ninth Circuit Decision

On appeal, the Ninth Circuit affirmed in part, reversed in part, and remanded. Turning first to the issues of direct infringement, the court first elaborated on the requirement of volitional conduct, citing its Giganews case and the Supreme Court's Aereo case, to conclude that "direct copyright liability for website owners arises when they are *actively involved* in the infringement" rather than engaged in passive participation.²¹⁰² "In other words, to demonstrate volitional conduct, a party like VHT must provide some 'evidence showing [the alleged infringer] exercised control (other than by general operation of [its website]); selected any material for upload, download, transmission, or storage; or instigated any copying, storage, or distribution' of its photos."²¹⁰³ The court concluded that VHT failed to satisfy that burden with respect to either the photos on the listing platform (the core of the web site, featuring photos and information about real estate properties) or on Digs.

With respect to photos on the listing platform, the court concluded that, on de novo review, it agreed with the district court's analysis and affirmed. The feed providers to the listing platform themselves selected and uploaded every photo, along with the evergreen or deciduous designations. As a result, the photos on the listing platform were not "selected" by Zillow. Nor did Zillow exercise control over those photos beyond the general operation of its web site. Zillow required feed providers to certify the extent of their rights to use each photo. Consistent with these designations, Zillow's system classified each photo as deciduous or evergreen and programmed its automated systems to treat each photo consistently with that scope of use certified by the third party. And when multiple versions of the same photo were submitted through the various feeds, Zillow invoked its copyright-protective "trumping" rules that gave preference to photos with evergreen rights over photos with deciduous rights in the same image. As the district court recognized, "trumping" was a reasonable way to design a system to manage multiple versions of the same photo when the authorized use varied across versions. Thus, Zillow had actively designed its system to avoid and eliminate copyright infringement.²¹⁰⁴

²¹⁰⁰ Id. at *49-50.

²¹⁰¹ Id. at *60-67.

²¹⁰² VHT, Inc. v. Zillow Group, Inc., 918 F.3d 723, 731-32 (9th Cir. 2019).

²¹⁰³ Id. at 732.

²¹⁰⁴ Id. at 733.

The court rejected VHT's argument that Zillow exhibited a conscious choice amounting to volitional conduct when it allegedly failed to remove photos once it received notice that infringing content was on the listing platform. The court noted that, to the contrary, once VHT put Zillow on notice of claimed infringement, Zillow took affirmative action to address the claims. The court therefore affirmed the district court's ruling that Zillow did not directly infringe VHT's copyrights in photos displayed on the listing platform post-sale.²¹⁰⁵

The court then turned to the district court's grant of JNOV with respect to direct infringement of 22,109 photos that were not displayed on Digs and 2,093 photos that were displayed by not searchable on Digs. First, the court rejected VHT's contention that the jury could have reasonably inferred that Zillow made "available for public display" all 22,109 of the "not displayed" photos. The court noted that VHT's contention presumed that the Copyright Act's display right encompasses an exclusive right to "make available for display," a position neither supported by the copyright statute nor embraced by the Ninth Circuit in the Perfect 10 v. Amazon case. But in any event, the court observed that VHT's argument based on a "make available" display right came too late, as the jury was never instructed on the "made available" theory. Thus, substantial evidence did not support a finding of direct infringement of VHT's public display rights in the 22,109 photos.²¹⁰⁶

The court then turned to the 2,093 photos that Digs users copied to "personal boards" and "Implicit Digs," but which Zillow did not add to the searchable set. A "personal board" was a digital bulletin board of images that a user saved or uploaded from the listing platform. Users could also upload their own images. These boards were typically private, though users could share a link to their boards. When a user saved a copy of an image with evergreen rights to a personal board, that image automatically joined a queue for review by a Zillow moderator. The moderator then decided whether to designate the photo for tagging so that it could be searchable on Digs, and thus select it for public display. Not all photos that were in the queue for moderation were reviewed. And in some instances, a user started but did not finish the process of saving an image to this board. Beginning in 2014, Zillow programmed these "clicked to save" images – called "Implicit Digs" – to enter the queue for moderator review in the same manner as if the photo had been saved to a personal board. The court rejected VHT's argument that the jury could have found that Zillow caused the 2,093 images to be displayed by subjecting the non-searchable VHT photo to the potential for moderation. The court found the argument defied logic because the only display that occurred was triggered by the user. Any potential for future display was purely speculative. The mere possibility that images might be moderated and tagged – conduct that is volitional – was not sufficient to transform Zillow from a passive host to a direct cause of the display of VHT's images.²¹⁰⁷

The court then considered VHT's reproduction and adaptation rights in the 2,093 displayed, non-searchable photos. The court concluded, following Giganews, that Zillow's

²¹⁰⁵ Id. at 733-34.

²¹⁰⁶ Id. at 736-37.

²¹⁰⁷ Id. at 737.

automated processes storing or caching VHT's photos were insufficiently volitional to establish that Zillow directly infringed VHT's reproduction and adaptation rights in the photos. Unlike photos that Zillow curated, selected, and tagged for searchable functionality – activities that amount to volitional conduct establishing direct liability – these 2,093 photos were copied to personal boards and Implicit Digs based on user actions, not the conduct of Zillow or its moderators. Nor was Zillow's behind-the-scenes technical work on Digs photos evidence that Zillow selected any material for upload, download, transmission or storage. Zillow produced cached copies of these Digs images, a process that automatically trimmed or padded images whose height and width did not match the target resolution, for the purposes of accelerating web site speed. This activity did not amount to volitional conduct. Nor could Zillow's promotion of Digs, including encouraging users to share photos through its site, be seen as instigating user copying. Zillow's conduct with respect to these photos was therefore, at most, passive participation in the alleged infringement and not sufficient to cross the volitional conduct line.²¹⁰⁸

The court next considered Zillow's appeal of the district court's summary judgment ruling that the searchable functionality of Digs did not constitute fair use as a matter of law (as a result of which the jury was allowed to consider fair use only with respect to the reproduction, cropping, and scaling of the 3,921 displayed, searchable photos).²¹⁰⁹ The focus of the parties' debate on this issue was whether Zillow's tagging of the 3,921 VHT photos for searchable functionality on Digs was transformative and thus supported a finding of fair use. The court first engaged in a review of the evolution of search engine cases involving assertions of transformative fair use. The court noted that, unlike the Internet-wide search engines considered in Perfect 10 v. Amazon and Kelly v. Arriba Soft, Digs was a closed-universe search engine that did not crawl the web. Users could run searches only on the searchable set of images within Digs' walled garden, which included VHT photos. The search results did not direct the user to the original sources of the photos, such as VHT's web site. Rather, they linked to other pages within Zillow's web site and, in some cases, to third party merchants that sold items similar to those featured in the photo. The court observed the fact that Digs made those images searchable did not fundamentally change their original purpose when produced by VHT – to artfully depict rooms and properties. In addition, Digs displayed the entire VHT image, not merely a thumbnail. Therefore, Zillow simply superseded VHT's purpose in creating the images in the first place. Unlike the Google Books search engine, the Zillow search system did not augment public knowledge and did nothing to further the use of copyrighted works for the socially valuable purposes enumerated in the fair use statute. The court therefore affirmed the district court's grant of summary judgment to VHT with respect to fair use.²¹¹⁰

The court ruled that the district court correctly granted JNOV to Zillow with respect to both contributory and vicarious infringement. Concerning contributory infringement, the court

²¹⁰⁸ Id. at 737-38.

²¹⁰⁹ Zillow did not appeal the jury's finding of direct infringement of those photos.

²¹¹⁰ Id. at 740-44.

recited the standard from Perfect 10 v. Visa that “contributory liability requires that a party ‘(1) has knowledge of another’s infringement and (2) either (a) materially contributes to or (b) induces that infringement.’”²¹¹¹ The court further quoted the articulation in Giganews that, in the online context, a computer system operator is liable under a material contribution theory of infringement if it has actual knowledge that specific infringing material is available using its system, and can take simple measures to prevent further damage to copyrighted works, yet continues to provide access to infringing works. The court found that in this case there was insufficient evidence to support the contributory infringement verdict under the “simple measures” standard.²¹¹²

Zillow testified throughout trial that, in order to systematically or swiftly take down a large number of photos, it required the Zillow Image ID – a number that was in the URL for each image. Merely identifying the physical property address in no way identified the proper feed or the correct photo. Thus, Zillow did not have appropriately specific information necessary to take simple measures to remedy the violation. The court rejected VHT’s argument that Zillow was liable for failing to ask for the URLs of the allegedly infringing photos, because asking for URLs was not Zillow’s duty under the contributory liability standard that it must have actual knowledge that specific infringing material is available using its system. The court noted Zillow first reasonably asked to see the licenses between VHT and the feed providers, because otherwise it could not assess ownership and rights in the undefined images. That Zillow did not proactively request a list of URLs before VHT filed suit did not make Zillow contributorily liable. Nor did Zillow induce infringement because it had not taken active steps, plainly and affirmatively communicated through words or actions, to encourage infringement.²¹¹³

With respect to the first prong of vicarious liability – the right and ability to supervise the infringing conduct – the court ruled the district court correctly found that Zillow lacked the practical ability to police its users’ infringing conduct on Digs. There was insufficient evidence that Zillow had the technical ability to screen out or identify infringing VHT photos among the many photos that users saved or uploaded daily to Digs. And under Perfect 10 v. Amazon, Zillow’s failure to change its operations to avoid assisting users to distribute infringing content was not the same as declining to exercise a right and ability to make third parties stop their direct infringement. The court therefore affirmed the district court’s JNOV concluding that substantial evidence did not support the claim that Zillow secondarily infringed VHT’s copyrights.²¹¹⁴

Finally, the court reversed the district court’s upholding of the jury’s finding that Zillow willfully infringed the copyrights in 2,700 searchable VHT photos that were eligible for statutory damages (the district court granted JNOV to Zillow on 673 images that were not displayed). The

²¹¹¹ Id. at 745 (quoting Perfect 10, Inc. v. Visa Int’l Serv. Ass’n, 494 F.3d 788, 795 (9th Cir. 2007)).

²¹¹² VHT, 918 F.3d at 745.

²¹¹³ Id. at 745-46.

²¹¹⁴ Id. at 746.

court noted that willfulness requires substantial evidence either that the infringing party was actually aware of the infringing activity or that the infringing party's actions were the result of reckless disregard for, or willful blindness to, the copyright holder's rights. Willful blindness requires that the infringing party subjectively believed that infringement was likely occurring on its networks and that it took deliberate actions to avoid learning about the infringement. With respect to actual notice, although VHT had provided Zillow with minimal notice of infringement (one letter with a list of allegedly infringing photos, designated by residential street address, not web address), the court noted that continued use of a work even after notification does not constitute willfulness so long as one reasonably and in good faith believes that he or she is not infringing. Such was the case here because Zillow's agreements with its feed providers granted it an express license to use, copy, distribute, publicly display, and create derivative works for each photo, and the agreements included unambiguous representations by the feed providers that they had the authority to assign such rights. Zillow had developed procedures to identify ex ante the scope of its license for each uploaded photo and employed automated protocols to manage the use of each photo consistent with its evergreen or deciduous designation. And after receiving the minimal notice letter from VHT, Zillow immediately requested information to confirm VHT's copyright ownership and cross reference the photos with licensing information, but VHT had not been forthcoming with the requested information.²¹¹⁵

With respect to reckless disregard or willfully blinding itself to infringement, the court rejected VHT's argument that Zillow, a sophisticated business with a robust legal team, should have known that its feed provider license agreements were invalid. VHT argued that when Zillow saw the non-exclusive grant of rights in VHT's unsigned form contract, showing that the feed providers did not have a right to sublicense, Zillow should have known the licenses were invalid. The court noted that despite requests for such information, Zillow did not have access to VHT's executed licenses with the feed providers who furnished VHT's photos to Zillow. Access to a blank form contract, which the district court had earlier found ambiguous as a matter of law, was insufficient. The court therefore concluded that substantial evidence did not show Zillow was reckless or willfully blind as to its infringement and vacated the jury's finding of willful infringement.²¹¹⁶

Finally, the court remanded for further proceedings on the size of the damages award, which hinged on whether VHT's photos used on Digs were part of a compilation or were individual photos. Because there were at least ten different copyright registrations, thousands of photos, and no explicit determination on compilation, the court declined to sort out the compilation issue on appeal.²¹¹⁷

The District Court's Decision on Remand

²¹¹⁵ Id. at 748-49.

²¹¹⁶ Id. at 749.

²¹¹⁷ Id. at 747-48.

On remand, the district court addressed two issues. First, based on the Supreme Court’s decision in the Fourth Estate case that copyright registration is made within the meaning of Section 411(a) not when an application for registration is filed, but when the Register has registered a copyright after examining a properly filed application,²¹¹⁸ Zillow moved for summary judgment and dismissal as to all copyright infringement claims on which Zillow was found liable because VHT had not secured registrations of its images as of the filing of the initial complaint, though it later amended its complaint after it had secured all the necessary registrations.²¹¹⁹

Noting that Section 411(a)’s registration requirement is not jurisdictional, the court rejected Zillow’s argument that it was required to dismiss VHT’s claims and could not excuse ZHT’s failure to secure registration as of the time of the complaint. The court declined to dismiss the claim on two grounds. First, it found that VHT’s excusal from compliance with Section 411(a) was law of the case because the fact that the case made it to trial implied a decision that VHT either complied with Section 411(a) or was excused from compliance. Second, even if the law of the case doctrine were inapplicable, the court ruled that it would excuse the registration requirement in this narrow instance where the case had proceeded as far as it had. The court noted that Zillow had cited no case in which a court dismissed copyright infringement claims based on Fourth Estate after a trial on the merits, a final judgment, an appeal, and a remand, and the court declined to do so here. The court found that no purposes behind Section 411(a)’s requirement would be served by vacating the final judgment and dismissing the case in its entirety.²¹²⁰

With respect to the statutory damages issue, the Ninth Circuit in its opinion in the appeal of this case read its prior precedents to mean that the question of whether something such as a photo or episode has independent economic value is not a “test,” but rather simply a non-dispositive factor that informs the analysis of whether a photo or episode is a separate “work” for purposes of statutory damages, and also does not resolve whether something is a “compilation” under the statutory definition of Section 101.²¹²¹ On remand, the district court went into some detail to reconcile the Ninth Circuit’s preceding statements with previous Ninth Circuit precedent on which the district court had relied in its judgment.

First, the district court noted that, if VHT’s images were each distinct “works” for statutory damages purposes (possibly by virtue of having, in part, independent economic value), it would appear they could not be a compilation, because a “compilation” is defined in the statute as a single “work” for statutory damages purposes. Second, the court read the Ninth

²¹¹⁸ Fourth Estate Public Benefit Corp. v. Wall-Street.com, LLC, 139 S. Ct. 881, 892 (2019).

²¹¹⁹ VHT, Inc. v. Zillow Grp., Inc., 461 F. Supp. 3d 1025, 1035 & n.6 (W.D. Wa. 2020).

²¹²⁰ Id. at 1037-40. The court also declined to exercise discretion to reconsider the judgment in view of Fourth Estate if it were considered an intervening change in law. The court concluded that Fourth Estate was not an intervening change in law with respect to VHT’s copyright claims in this case because Fourth Estate was decided after trial and judgment but before the appellate opinion in this case, and the issue was not raised on appeal. Id. at 1039.

²¹²¹ Id. at 1042.

Circuit’s instruction to focus on the statutory definition of “compilation” and the text of the definition itself to require it to consider how VHT’s images were “selected, coordinated, or arranged” in analyzing whether they constituted a compilation.²¹²² The court found persuasive the method of determining whether something is a compilation elaborated in the Second Circuit’s decision in *Bryant v. Media Right Prods., Inc.*,²¹²³ in which the Second Circuit focused on whether the copyright holder issued its works separately, or together as a unit. The district court noted that, under that analysis, it might be possible for materials to have independent economic value if issued separately (and therefore potentially constitute separate “works”), but in fact not be issued separately (and therefore constitute a compilation). In sum, the court found the most faithful reading of the Ninth Circuit’s opinion in this case to be that prior Ninth Circuit precedent was about “works,” not “compilations.” The *Bryant* test could therefore be reconciled with Ninth Circuit precedent by interpreting it as defining a “compilation,” separate and apart from a “work.”²¹²⁴

Applying the preceding analysis, the district court agreed with VHT that the germane question here was not whether it stored its photos in a master photo database, because VHT’s organization of its images prior to issuance did not answer the question of how VHT’s images were organized or arranged when issued. VHT argued instead that the question was whether the “works infringed” made up a compilation or not. The court agreed with VHT, and noted that in fact VHT licensed its images on a per-image or per-property basis. Although the fact that VHT group-registered its images as “compilations” weighed in favor of a “compilation” finding, that fact was not controlling, and the court found it outweighed by the form in which VHT issued its images. Finally, to the extent the images’ independent economic value remained a factor to consider in the “compilation” analysis, the court concluded, based on the jury’s finding that each image had independent economic value when awarding statutory damages, this factor weighed against finding a “compilation.” Accordingly, the court granted VHT’s motion for summary judgment that it was entitled to a separate statutory damages award for each remaining image in the case.²¹²⁵

The Ninth Circuit Decision

On appeal, the Ninth Circuit affirmed the district court’s decision in full, holding that the district court correctly concluded that the registration of the photos as a database did not automatically limit statutory damages to a single award when multiple photos in the database had been infringed. VHT licensed the individual photos in the database, not the database itself, and the database itself was not published. Zillow used each photo independently to market home designs. It was not selecting photos on the authorship or arrangement of the photos within the database. Instead, it obtain images from feed providers based on the photos

²¹²² *Id.* at 1043-44.

²¹²³ 603 F.3d 135 (2d Cir. 2010).

²¹²⁴ *VHT*, 461 F. Supp. 3d at 1044.

²¹²⁵ *Id.* at 1045.

themselves. Zillow infringed the individual photos, not the database. And the individual infringed photos were not in any way selected, coordinated, or arranged to create an original work of authorship. Accordingly, the infringed works were not the database but instead the 2,700 individual photographs, and VHT was entitled to an award for each of the 2,700 infringements.²¹²⁶

(j) Atari v. Redbubble

The defendant Redbubble provided an online marketplace where independent artists could upload their designs and creative works for printing on a range of products selected by users of the site, including apparel, stationery, housewares, bags, stickers, and wall art. Users were able to customize both the physical form of the product as well as the design to be placed upon it. Redbubble then forwarded the order to a preselected third party manufacturer that created the final product based on the customer's specifications. Artists uploaded their art designs to Redbubble and selected, from a list predetermined by Redbubble, the products on which the art could be sold. Redbubble set a base price that covered its fee and manufacturing costs, while the artist selected the margin that he or she would receive from the sale. None of the artist, customer, or manufacturer interacted with each other – all communicated exclusively through Redbubble. The final product was shipped to the customer in Redbubble packaging and the customer was directed to Redbubble's web site to address any issues.²¹²⁷

The plaintiff Atari discovered that Redbubble carried its trademarked and copyrighted designs and filed a complaint for copyright and trademark infringement, asserting claims for direct, contributory and vicarious copyright liability. After the complaint was filed, Redbubble immediately removed the listings identified in Atari's complaint and began to proactively police for Atari-related designs. The parties disputed its success in these efforts – Atari experts identified over 4,000 repeat offenders who had uploaded Atari designs, including some artists that were reported for infringement six or more times before being suspended from the Redbubble site. The parties filed cross motions for summary judgment.²¹²⁸

With respect to direct liability, the court analyzed whether Atari had established causation in the form of the volitional conduct requirement. The court found insufficient volitional conduct on Redbubble's part with respect to Atari's display rights because Redbubble did not exercise control other than by general operation of its web site with respect to displays of Atari's designs. Although Redbubble arguably modified the infringing image it received from artists by applying them to stock photos of physical goods such as apparel, those acts did not demonstrate the type of control that would support direct liability. Any modification occurred automatically with no intervening act by Redbubble employees. Nor did Redbubble select any material for upload, download, transmission or storage – those acts were performed by the web site's users. Redbubble exercised no control or selection over infringing designs and could not

²¹²⁶ VHT, Inc. v. Zillow Grp., Inc., 69 F.4th 983, 986, 990, 993 (2023).

²¹²⁷ Atari Interactive, Inc. v. Redbubble, Inc., 515 F. Supp. 3d 1089, 1096-98 (N.D. Cal. 2021).

²¹²⁸ Id. at 1095, 1098-99.

stop them from being uploaded. Nor did it initiate the display of infringing images, which occurred automatically in response to user actions.²¹²⁹

However, the court found a question of material fact in whether Redbubble instigated any copying, storage or distribution of infringing images. The court noted that Redbubble held itself out as the seller of the goods on its web site. It offered those items for sale and then facilitated or caused their creation and delivery, with no involvement from the artists who uploaded the designs.²¹³⁰ The court stated, “Even though each step is performed automatically by a computer, the acts remain volitional because Redbubble designed its software to accomplish those tasks and for its own financial benefit.”²¹³¹ Moreover, the court noted that Redbubble exercised control over every aspect of the sale, from manufacturing to shipping and returns, and thus held the best position to prevent infringement. The court therefore concluded that a reasonable jury could find Redbubble liable for direct infringement, and accordingly denied both parties’ motions for summary judgment as to Atari’s claim for copyright infringement.²¹³²

With respect to contributory liability, the court noted that contributory liability requires a showing that the defendant (1) has knowledge of another’s infringement and (2) either (a) materially contributes to or (b) induces that infringement. The defendant must know of specific infringing material and fail to take simple measures to prevent further damage. The court observed, however, that the law remains unsettled over whether “reason to know” of specific infringement satisfies the standard. The court found that, regardless of the precise standard for knowledge required, Atari had failed to satisfy it. Atari provided no evidence that Redbubble knew of specific infringing material and failed to act. Atari relied on broad willful blindness claims due to alleged widespread infringement on Redbubble’s web site. The court ruled that such reliance was insufficient. Generalized knowledge of infringement might support liability only if Redbubble failed to take reasonable steps to prevent infringement, but that was not what the record showed. Atari had neither identified affirmative steps that Redbubble took to avoid learning of infringement nor showed that Redbubble’s moderation policies were unreasonable. Accordingly, Redbubble was entitled to summary judgment on the contributory infringement claim.²¹³³

With respect to vicarious infringement, the court noted that vicarious liability requires that the defendant have (1) the right and ability to supervise the infringing conduct and (2) a direct financial interest in the infringing activity.²¹³⁴ After reviewing the VHT (discussed in

²¹²⁹ Id. at 1112-13.

²¹³⁰ Id. at 111.3

²¹³¹ Id.

²¹³² Id.

²¹³³ Id. at 1114-15.

²¹³⁴ Id. at 1115.

Section III.C.1(i) below) and Napster (discussed in Section III.C.2(c)(1) below) cases, the court ruled as follows:

On balance, Redbubble is closer to VHT than to Napster. Read together, the cases require a relatively close relationship between the means for finding infringement (music index, image URL, etc.) and the infringing content. Here, search terms for particular brands would presumably find infringing content because, as in Napster, artists would tag the infringing content to enable users to find it. However, the keywords would also find a variety of non-copyrighted or fair use content that happened to be tagged with the brand. For example, Redbubble shows that a search for “Atari” on Redbubble produces designs of pixelated graphics, game controllers, Isle of Dogs tshirts, “I love the 90s” stickers, and a variety of references [to] old-school gaming. Also, depending on the keywords submitted by artists, word searches might be ineffective in identifying some infringing content. Moreover, Redbubble introduces evidence that it lacks ability to monitor infringing images and that it requires cooperation from the content owner to determine whether particular content infringes.

On these facts, the Court agrees that finding infringement would be like “searching for a needle in a haystack” (where Redbubble lacks knowledge of needles’ appearance). Atari therefore cannot establish vicarious copyright infringement, and Redbubble is entitled to judgment.²¹³⁵

Finally, Redbubble asserted that it was protected from liability by the Section 512(c) safe harbor of the DMCA (for discussion of this safe harbor and cases adjudicating it, see Section III.C.6(b)(1)(iii) below). The parties disputed whether Redbubble’s use of the artists’ uploaded images satisfied the “by reason of storage” requirement of Section 512(c). Atari contended that Redbubble’s volitional acts in copying infringing designs onto model photos to create images of products for sale, and exhibiting those images on Redbubble’s product pages that were hosted on its web site, distinguished Redbubble from a service provider that merely provides a platform to which a third party uploads infringing material. Redbubble responded that, like the Amazon Marketplace software, the Redbubble platform software performed functions for the purpose of facilitating access to the listings uploaded by third-party sellers, and therefore satisfied the requirement.²¹³⁶

The court noted that there appeared to be little authority on point. The cases Redbubble cited as extending DMCA immunity from suit did not even discuss the “by reason or storage” element and Redbubble cited no authority finding a failure to establish that element on similar facts. Nevertheless, the court concluded that Redbubble had failed to satisfy the element. The images on its web site were not stored “at the direction of the user” because Redbubble actively participated in modifying the files uploaded by users to display the designs on Redbubble-

²¹³⁵ Id. at 1116.

²¹³⁶ Id. at 1114.

selected physical products. Redbubble was therefore not entitled to the Section 512(c) safe harbor.²¹³⁷

2. Contributory Liability

Under the traditional formulation of contributory liability, a party may be liable for contributory infringement where “with knowledge of the infringing activity, [it] induces, causes or materially contributes to the infringing activity of another.”²¹³⁸ The standard of knowledge is objective: to know or have reason to know that the subject matter is copyrighted and that the particular uses were violating copyright law.²¹³⁹ In the Grokster case, the Supreme Court stated that “For liability for contributory infringement, there must be a direct infringement to which the contributory infringer has knowledge and encourages or facilitates.”

The requirement of knowledge may eliminate contributory liability on the part of an OSP or BBS operator with respect to many instances of infringement for which the OSP or BBS is merely a passive information conduit and has no knowledge of the infringement. However, given knowledge (or reason to know), a number of cases suggest that a system provider cannot simply continue to provide the facility that enables infringement.

(a) The Netcom Case

In Religious Technology Center v. Netcom On-Line Communication Services,²¹⁴⁰ the court held that the OSP Netcom could be contributorily liable for infringing postings by an individual named Erlich of copyrighted religious materials to Usenet through the provider after the service was given notice of the infringing material. “If plaintiffs can prove the knowledge element, Netcom will be liable for contributory infringement since its failure to simply cancel Erlich’s infringing message and thereby stop an infringing copy from being distributed worldwide constitutes substantial participation in Erlich’s public distribution of the message.”²¹⁴¹ The court held that the copyright notices in the posted works were sufficient to give Netcom notice that the works were copyrighted.²¹⁴²

²¹³⁷ Id.

²¹³⁸ E.g., Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971); Cable/Home Communications Corp. v. Network Prods., Inc., 902 F.2d 829, 845 (11th Cir. 1990).

²¹³⁹ R. Nimmer, *Information Law* ¶ 4.11, at 4-40 (2001); see also Sega Enterprises Ltd. v. MAPHIA, 948 F. Supp. 923, 933 (N.D. Cal. 1996) (“The standard for the knowledge requirement is objective, and is satisfied where the defendant knows or has reason to know of the infringing activity.”) (citing Casella v. Morris, 820 F.2d 362, 365 (11th Cir. 1987)).

²¹⁴⁰ 907 F. Supp. 1361 (N.D. Cal. 1995).

²¹⁴¹ Id. at 1374.

²¹⁴² Id.

However, the court was careful to note that where an operator is unable to verify a claim of infringement, there may be no contributory liability:

Where a BBS operator cannot reasonably verify a claim of infringement, either because of a possible fair use defense, the lack of copyright notices on the copies, or the copyright holder's failure to provide the necessary documentation to show that there is a likely infringement, the operator's lack of knowledge will be found reasonable and there will be no liability for contributory infringement for allowing the continued distribution of the works on its system.²¹⁴³

Nevertheless, the court clearly imposed a duty on the operator to actively attempt to verify a claim of infringement and to take appropriate action in response:

Thus, it is fair, assuming Netcom is able to take simple measures to prevent further damage to plaintiffs' copyrighted works, to hold Netcom liable for contributory infringement where Netcom has knowledge of Erlich's infringing postings yet continues to aid in the accomplishment of Erlich's purpose of publicly distributing the postings.²¹⁴⁴

(b) The MAPHIA Case

In addition to the Netcom case, the court in the subsequent MAPHIA case²¹⁴⁵ (also out of the Northern District of California) held a BBS and its system operator liable for contributory infringement for both the uploading and the subsequent downloading of copies of Sega's video games by users where the system operator had knowledge that the infringing activity was going on through the bulletin board, and had specifically solicited the uploading of the games for downloading by users of the bulletin board. The court cited the Ninth Circuit's decision in Fonovisa, Inc. v. Cherry Auction, Inc.²¹⁴⁶ for the proposition that providing the site and facilities for known infringing activity is sufficient to establish contributory liability. "In this case, Sherman provided the BBS as a central depository site for the unauthorized copies of games, and allowed subsequent distribution of the games by user downloads. He provided the facilities for copying the games by providing, monitoring, and operating the BBS software, hardware, and phone lines necessary for the users to upload and download games."²¹⁴⁷ This suggests that mere operation of a BBS, at least if the operator knows that infringing activity is taking place, may be sufficient for contributory liability.

²¹⁴³ Id.

²¹⁴⁴ Id. at 1375.

²¹⁴⁵ Sega Enterprises Ltd. v. MAPHIA, 948 F. Supp. 923 (N.D. Cal. 1996).

²¹⁴⁶ 76 F.3d 259 (9th Cir. 1996).

²¹⁴⁷ MAPHIA, 948 F. Supp. at 933.

However, the court went on to hold that Sherman would have been liable as a contributory infringer even under a higher standard requiring more direct participation in the infringement that the court believed the Netcom decision established:

However, even under an alternative and higher standard of “substantial participation,” Sherman is liable. Under this standard, Sherman is only liable if he knew of the users’ infringing actions, and yet substantially participated by inducing, causing or materially contributing to the users’ infringing conduct. Netcom, 907 F. Supp. at 1382. In this case, Sherman did more than provide the site and facilities for the known infringing conduct. He actively solicited users to upload unauthorized games, and provided a road map on his BBS for easy identification of Sega games available for downloading. Additionally, through the same MAPHIA BBS medium, he offered copiers for sale to facilitate playing the downloaded games.²¹⁴⁸

(c) The Peer-to-Peer Filing Sharing Cases

(1) The Napster Cases

In December of 1999, the Recording Industry Association of America, Inc. (RIAA), on behalf of 18 of its members, filed a complaint in federal court in the Northern District of California for contributory and vicarious copyright infringement against Napster, Inc., the operator of a Web site (www.napster.com) designed to enable its members to locate music files in the MP3 format²¹⁴⁹ stored on the hard disks of other members, and to initiate downloads of such files through a “peer-to-peer” architecture – i.e., transfers directly from the computer of one user to the computer of another user without passing through the Napster servers.

1. Factual Background. Napster offered to its members a piece of proprietary software called “MusicShare” for download from its website free of charge. When a Napster user logged on, the MusicShare software would interact with the Napster server software to connect the user to one of many servers operated by Napster, would read a list of names of MP3 files that the user had elected to make available on his or her personal computer for sharing with other users (by placing them in certain designated directories on his or her hard disk known as the “user library”), and would then store the names of those files in an index maintained on the Napster server. Once the file names were successfully uploaded to the index, each user library, identified by a user name, would become a “location” on the Napster servers. Napster locations were short-lived – they were respectively added or purged every time a user signed on or off of

²¹⁴⁸ Id. The court further held that because Sega had established contributory liability on the part of Sherman, the court need not address whether Sherman was also liable under the theory of vicarious liability. Id.

²¹⁴⁹ MP3 stands for Motion Picture Expert Group 1, Audio Layer 3. MP3 is an algorithm that compresses a digital music file by a ratio of approximately 12:1, thereby reducing the size of the file so that it more easily and quickly can be downloaded over the Internet. A&M Records Inc. v. Napster Inc., 54 U.S.P.Q.2d 1746, 1747 n.1 (N.D. Cal. 2000).

the network. Thus, a particular user's MP3 files designated for sharing would be accessible to other users only while that user was online.²¹⁵⁰

An account holder could use the search tools included in the MusicShare software to find MP3 files being shared by other users by searching the index containing the names of MP3 files that online users saved in their designated user library directories. Users wishing to search for a song or artist could do so by entering the name of the song or artist in the search fields of the MusicShare software and then clicking a "Find It" button. The Napster servers would perform a text search of the file names in the index and respond by sending the requesting user a list of files that included the same term(s) the requesting user entered on the search form. Alternatively, users could access MP3 files via a "hotlist" function. This function enabled a Napster user to archive other user names and learn whether account holders who accessed the network under those names were online. A requesting user could access or browse all files listed in the user libraries of hotlisted users.²¹⁵¹

In either case, once a requesting user located and selected a desired file from a list of search results or a list of files made available by a hotlisted user, the Napster server software would then engage in a dialog with the MusicShare software of the requesting user and that of the "host user" (i.e., the user who made the desired MP3 file available for downloading). The Napster server would obtain the necessary Internet Protocol (IP) address information from the host user, communicate the host user's address or routing information to the requesting user, and the requesting user's computer would then employ this information to establish a "peer-to-peer" connection directly with the host user's MusicShare software and download the MP3 file from the host user's library. The content of the actual MP3 file would be transferred over the Internet between the users, not through the Napster servers. No MP3 music files were stored on the Napster servers themselves.²¹⁵²

The plaintiffs, owners of the copyrights in many of the sound recordings being downloaded by users through the Napster system, brought claims for contributory and vicarious copyright infringement and sought a preliminary injunction against Napster. A second, very similar case, was filed against Napster in federal district court in the Northern District of California on Jan. 7, 2000.²¹⁵³ That case was a class action filed by named plaintiffs Jerry Leiber, Mike Stoller, and Frank Music Corp. on behalf of themselves and "those music publisher-principals of The Harry Fox Agency, Inc."²¹⁵⁴ The complaint alleged that Napster's Web site constituted inducement and contributory infringement of the copyrights in various musical compositions held by the members of the class.²¹⁵⁵ The complaint further alleged that Napster

²¹⁵⁰ A&M Records Inc. v. Napster Inc., 114 F. Supp. 2d 896, 905 (N.D. Cal. 2000).

²¹⁵¹ Id. at 906.

²¹⁵² Id. at 907.

²¹⁵³ Leiber et al. v. Napster Inc., No. C 00 0074 ENE (N.D. Cal. Jan. 7, 2000).

²¹⁵⁴ Id. ¶ 10.

²¹⁵⁵ Id. ¶¶ 1, 29.

was contributing to the unauthorized reproduction and distribution of “phonorecords” embodying the copyrighted musical compositions of members of the class without obtaining the necessary authority from The Harry Fox Agency.²¹⁵⁶ Those two cases were consolidated before Judge Marilyn Hall Patel.

Several other copyright holders, including the artists Metallica and Dr. Dre and several independent recording artists and labels, as well as the Academy of Motion Picture Arts and Sciences (AMPAS), ultimately also filed lawsuits against Napster for copyright infringement, all of which were eventually consolidated before Judge Patel in the Northern District of California under the Multi-District Litigation (MDL) rules of the federal courts. In July of 2000, the district court entered a broad preliminary injunction against Napster. Before it took effect, however, the Ninth Circuit stayed the injunction pending an expedited appeal by Napster.

After appeal, the Ninth Circuit issued an opinion affirming in part and reversing in part, with a remand to the district court to enter a modified preliminary injunction of narrower scope, which the district court did on Mar. 5, 2001. Both sides filed a second appeal to the Ninth Circuit based on the Mar. 5 preliminary injunction. The Mar. 5 order was clarified by the district court in a memorandum dated Apr. 26, 2001, then orally modified by the court from the bench on July 11, 2001. Ten days before the oral modification of the injunction, on July 1, 2001, Napster voluntarily suspended file sharing through its service. On July 18, 2001, the Ninth Circuit stayed the district court’s July 11 oral modification of the preliminary injunction. Both Napster and the plaintiffs pursued further appeals to the Ninth Circuit in view of the July 11 oral order. The Ninth Circuit consolidated those appeals with the earlier appeals of the Mar. 5 modified injunction.

The Napster cases raised a number of issues of significant importance to online copyright law, and the district court and the Ninth Circuit took somewhat different approaches with respect to various of the issues. With respect to each issue, the district court’s analysis will first be described, followed by the Ninth Circuit’s analysis of the issue. Because there were multiple appeals to the Ninth Circuit, the first opinion issued by the Ninth Circuit will be referred to as “Napster I,” to distinguish it from the later opinion issued by the Ninth Circuit as a result of the subsequent consolidated appeals, which will be referred to as “Napster II.”

2. Whether Any Otherwise Direct Infringement by Napster’s Users Was Immunized by the AHRA. The district court ruled that Napster was both contributorily and vicariously liable for infringing downloads of copyrighted material by its users via the Napster system. The court ruled that the plaintiffs had established a prima facie case of direct copyright infringement by Napster users because “virtually all Napster users engage in the unauthorized downloading or uploading of copyrighted music; as much as eighty-seven percent of the files available on Napster may be copyrighted, and more than seventy percent may be owned or administered by plaintiffs.”²¹⁵⁷ The Ninth Circuit in Napster I agreed, concluding that (i) the mere uploading of file names to the search index by Napster users, thereby making the files corresponding to those file

²¹⁵⁶ Id. ¶ 30.

²¹⁵⁷ Napster, 114 F. Supp. 2d at 911.

names *available* for downloading (whether or not they were in fact downloaded by other users) constituted an infringement of the plaintiffs' exclusive distribution rights and (ii) the unauthorized downloading of files containing copyrighted music by Napster users violated the plaintiffs' exclusive reproduction rights.²¹⁵⁸

Napster argued that its users' downloads of music for their own personal use were immunized by the Audio Home Recording Act of 1992 (AHRA).²¹⁵⁹ The AHRA made two major substantive changes to copyright law. First, Subchapter D of the AHRA (Section 1008) immunizes certain noncommercial recording and use of musical recordings in digital or analog form.²¹⁶⁰ Section 1008 provides:

No action may be brought under this title alleging infringement of copyright²¹⁶¹ based on the manufacture, importation, or distribution of a digital audio recording device, a digital audio recording medium, an analog recording device, or an analog recording medium, or based on the noncommercial use by a consumer of such a device or medium for making digital musical recordings or analog musical recordings.

Second, Subchapters B and C (Sections 1002-1007) of the AHRA require (i) that any "digital audio recording device" conform to the "Serial Copyright Management System" (SCMS), which allows unlimited first generation copies of an original source, but prohibits second generation copies (i.e., copies of a copy), and (ii) that manufacturers and distributors of digital audio recording devices and digital audio recording media (such as DAT tape and recordable CDs) pay royalties and file various notices and statements to indicate payment of those royalties.²¹⁶²

Napster argued that under the direct language of Section 1008, no action for infringement of copyright could be brought against Napster's users, who were consumers and who were engaged in the noncommercial making and sharing (distribution) of digital musical recordings. Because the actions of Napster's users were immune, Napster argued that it could not be contributorily or vicariously liable for those actions.²¹⁶³ Napster cited the following legislative history of the AHRA as support for its argument that Congress intended to afford a very broad immunity for non-commercial copying of audio recordings:

²¹⁵⁸ *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1014 (9th Cir. 2001) ("Napster I").

²¹⁵⁹ Pub. L. No. 102-563, 106 Stat. 4244 (1992), codified at 17 U.S.C. §§ 1001-1010.

²¹⁶⁰ *Nimmer* § 8B.01 (2000).

²¹⁶¹ The immunity applies with respect to copyrights in both the sound recordings and any musical compositions embodied therein. *Id.* § 8B.07[C][2], at 8B-90.

²¹⁶² *Id.* §§ 8B.02 & 8B.03 (2000).

²¹⁶³ Opposition of Defendant Napster, Inc. to Plaintiffs' Motion for Preliminary Injunction, *A&M Records, Inc. v. Napster, Inc.*, Civ. Nos. C99-5183 MHP (ADR) & C00-0074 MHP (ADR) (July 5, 2000), at 5-6 (hereinafter, "Napster's PI Opp. Br."), on file with the author.

- S. Rep. 102-294 (1992) at 51 (“A central purpose of the Audio Home Recording Act of 1991 is conclusively to resolve [the] debate” over the “copyright implications of private audio recording for noncommercial use.”).
- H. Rep. 102-873(I) (1992) at 24 (“In the case of home taping, the exemption protects all noncommercial copying by consumers of digital and analog musical recordings.”).
- Contemporaneous comments by Jason Berman, former head of the RIAA, acknowledging that the immunity provisions of the AHRA were intended to have a broad scope, stating: “The [AHRA] will eliminate the legal uncertainty about home audio taping that has clouded the marketplace. The bill will bar copyright infringement lawsuits for both analog and digital home audio recording by consumers” H.R. 4567, Serial No. 102-139 (March 1992).
- Comments by Senator DeConcini, who was influential in passing the AHRA: “[The AHRA] makes clear the private, non-commercial taping, of both analog and digital material, is permissible under the copyright law. As new and improved technologies become available, such clarification in the law becomes more important.” 137 Cong. Rec. S11845 (1992).²¹⁶⁴

Napster also cited a report by the Office of Technology Assessment (OTA) on home taping as evidence that Congress, in enacting the AHRA, fully understood that consumers would share music with family, friends and others. In particular, the OTA report deemed taping CDs or records borrowed from friends, and giving copies of one’s own CDs or records to friends, to be synonymous with “personal use,” “private copying,” “home use,” and “private use.”²¹⁶⁵ The OTA report noted that, even by 1989, copying for personal use was widespread: 37% of the home tapers surveyed copied music they borrowed from a friend or other family members; 26% gave away the last copy they made to others outside their household or to family members; and 41% had within the last year borrowed a friend’s music to copy so they would not have to buy it themselves.²¹⁶⁶ Napster argued that Congress had knowingly legislated a very broad form of immunity for all of this conduct.²¹⁶⁷

Finally, Napster argued that the Ninth Circuit’s decision in Recording Indus. Ass’n of Am. v. Diamond Multimedia Sys.²¹⁶⁸ supported its argument that the AHRA immunized the sharing of musical recordings by Napster’s users. At issue in that case was whether the “Rio” device, a small device with headphones that allowed a user to download MP3 files from a computer hard

²¹⁶⁴ Id. at 6.

²¹⁶⁵ U.S. Congress, OTA, *Copyright and Home Copying: Technology Challenges the Law*, OTA-CIT-422, at 5, 156 (U.S. GPO, Oct. 1989).

²¹⁶⁶ Id. at Tables 6-10, 6-12 at 270 & Table 7-4 at 274.

²¹⁶⁷ Napster’s PI Opp. Br., *supra* note 2163, at 6-7.

²¹⁶⁸ 180 F.3d 1072 (9th Cir. 1999).

drive and listen to them elsewhere, was a “digital audio recording device” subject to the SCMS requirements of the AHRA. The Ninth Circuit held that it was not, on the following rationale. A “digital audio recording device” is defined as a device having a digital recording function whose primary purpose is to make a “digital audio copied recording,” which is defined as a reproduction of a “digital musical recording.” 17 U.S.C. § 1001(1), (3). However, a “digital musical recording” is defined to *exclude* a material object “in which one or more computer programs are fixed.” *Id.* § 1001(5)(B)(ii). The Ninth Circuit ruled that a computer hard drive falls within this exemption, and therefore that MP3 files stored on a hard drive do not constitute a “digital musical recording.”²¹⁶⁹ Because the Rio did not make copies from “digital musical recordings,” it was not a “digital audio recording device” and was therefore not subject to the SCMS requirements of the AHRA.²¹⁷⁰

As support for its decision, the Ninth Circuit stated the following about the immunity provisions of the AHRA:

In fact, the Rio’s operation is entirely consistent with the [AHRA’s] main purpose – the facilitation of personal use. As the Senate Report explains, “[t]he purpose of [the] Act is to ensure the right of consumers to make analog or digital recordings of copyrighted music for their private, noncommercial use.” The Act does so through its home taping exemption, see 17 U.S.C. § 1008, which “protects all noncommercial copying by consumers of digital and analog musical recordings.” The Rio merely makes copies in order to render portable, or “space-shift,” those files that already reside on a user’s hard drive.”²¹⁷¹

Napster argued that in the preceding passage from the Diamond decision, the Ninth Circuit had ruled that Section 1008 of the AHRA gives a consumer the right to create personal MP3 files, and that copying a music file from one’s hard drive to a portable device was also appropriate. Napster concluded that, if a consumer can copy an MP3 file from his or her hard drive without violating the copyright laws, Napster’s directory service did not violate the copyright laws either.²¹⁷²

In response, the plaintiffs argued that, because Section 1008 states that no action for infringement may be brought based on “the noncommercial use by a consumer of *such a device* [i.e., a digital audio recording device] ... for making digital musical recordings” (emphasis added), and because the Ninth Circuit held in Diamond that a computer hard drive is not a “digital audio recording device,” the immunity of Section 1008 does not extend to MP3 files stored on a computer hard drive. The Napster case, then, presented an issue of first impression of whether

²¹⁶⁹ *Id.* at 1078.

²¹⁷⁰ *Id.* at 1078-79.

²¹⁷¹ *Id.* at 1079 (citations omitted).

²¹⁷² Napster’s PI Opp. Br., *supra* note 2163, at 5-6.

the definitions of Section 1001 should be read to limit *both* the scope of the SCMS/royalty requirements *and* the scope of the immunity of the AHRA.²¹⁷³

The district court, in a terse analysis of the AHRA in a footnote, rejected the argument that Section 1008 of the AHRA immunized the actions of Napster's users for two reasons. First, the court ruled that the "AHRA is irrelevant to the instant action" because "[n]either the record company nor music publisher plaintiffs have brought claims under the AHRA."²¹⁷⁴ Second, the court labeled the passage from Diamond quoted above and cited by Napster as "dicta" and found it to be "of limited relevance":

The *Diamond Multimedia* court *did* opine that making copies with the Rio to space-shift, or make portable, files already on a user's hard drive constitutes "paradigmatic noncommercial personal use entirely consistent with the purposes of the Act [i.e. the facilitation of personal use]." However, this dicta is of limited relevance. Because plaintiffs have not made AHRA claims, the purposes and legislative history of the AHRA do not govern the appropriateness of a preliminary injunction against Napster, Inc. Furthermore, as explained below, the court is not persuaded that space-shifting constitutes a substantial, noninfringing use of the Napster service. The Ninth Circuit did not discuss the fair use doctrine in *Diamond Multimedia*.²¹⁷⁵

On appeal in Napster I, the Ninth Circuit affirmed the conclusion that the AHRA did not immunize the activities of Napster users in sharing audio files, although on a different rationale from the district court. The Ninth Circuit did not endorse the district court's rationale that the AHRA was inapplicable merely because the plaintiffs had not brought claims under the AHRA. Instead, the Ninth Circuit cited its rulings in Diamond that computers and their hard drives are not "digital audio recording devices" and that computers do not make "digital musical

²¹⁷³ Prof. Nimmer notes that the Ninth Circuit's Diamond decision could be read to mean that the immunity provisions of the AHRA are not limited by that Court's own construction of the definitions of the technical terms that it held to limit the scope of the SMCS/royalty requirements: "Based on the legislative history's characterization of 'all noncommercial copying by consumers of digital and analog musical recordings' as falling under the protection of the home taping exemption, the court appears ready to apply that provision beyond its precise wording." *Nimmer* § 8B.07[C][4], at 8B-94.

Napster also argued that a narrow application of § 1008 would lead to the absurd construction that a manufacturer of a device capable of copying a CD (which is clearly a digital musical recording) onto a hard drive would be immune, yet when a consumer used that very same device to copy her musical recording from the hard drive back onto a CD or onto a Rio for her own or a friend's personal use, she would not have immunity. Napster argued that constructions of statutory language that lead to absurd results clearly contrary to legislative intent must be rejected, citing *United Steel Workers v. Weber*, 443 U.S. 193, 204 (1979); *Train v. Colorado Public Interest Research Group*, 426 U.S. 1, 7 (1975); *Ozawa v. United States*, 260 U.S. 178, 194 (1922). Napster's PI Opp. Br., *supra* note 2163, at 8 n.8.

²¹⁷⁴ Napster, 114 F. Supp. 2d at 915 n.19.

²¹⁷⁵ *Id.* (citations omitted; emphasis in original).

recordings,” as those terms are defined in the AHRA. Accordingly, the AHRA does not cover the downloading of MP3 files to computer hard drives.²¹⁷⁶

3. The Fair Use Doctrine Generally. Napster also contended that its users did not directly infringe plaintiffs’ copyrights because the users were engaged in a noncommercial, fair use of the materials. The district court rejected this argument, ruling that the downloading of musical recordings through Napster did not qualify generally under the four fair use factors. With respect to the first factor – the purpose and character of the use – the district court held that downloading MP3 files was not transformative and, although Napster did not charge for its service, was commercial in nature:

Although downloading and uploading MP3 music files is not paradigmatic commercial activity, it is also not personal use in the traditional sense. Plaintiffs have not shown that the majority of Napster users download music to sell – that is, for profit. However, given the vast scale of Napster use among anonymous individuals, the court finds that download and uploading MP3 music files with the assistance of Napster are not private uses. At the very least, a host user sending a file cannot be said to engage in a personal use when distributing that file to an anonymous requester. Moreover, the fact that Napster users get for free something they would ordinarily have to buy suggests that they reap economic advantages from Napster use.²¹⁷⁷

The Ninth Circuit affirmed this ruling in Napster I, agreeing with the district court that the downloading was not transformative, and that Napster users were engaging in commercial use of the copyrighted materials because (i) users could not be said to be engaged in a “personal use” when distributing a file to an anonymous requester and (ii) Napster users get something for free they would ordinarily have to buy.²¹⁷⁸ “Direct economic benefit is not required to demonstrate a commercial use. Rather, repeated and exploitative copying of copyrighted works, even if the copies are not offered for sale, may constitute a commercial use.”²¹⁷⁹ Because the record demonstrated that Napster users’ repeated copying was made to save the expense of purchasing authorized copies, such uses were commercial, causing the first factor to weigh in favor of plaintiffs.²¹⁸⁰

The district court held that the second factor – nature of the copyrighted work – weighed against fair use because the copyrighted sound recordings and compositions at issue were creative in nature. The third factor – amount and substantiality of the portion used in relation to the whole – also weighed against fair use because copies of entire works were being

²¹⁷⁶ Napster I, 239 F.3d at 1024-25.

²¹⁷⁷ Napster, 114 F. Supp. 2d at 912.

²¹⁷⁸ Napster I, 239 F.3d at 1015.

²¹⁷⁹ Id.

²¹⁸⁰ Id.

downloaded.²¹⁸¹ Finally, the district court found that the fourth factor – the effect on the potential market for the copyrighted work – weighed against fair use because the plaintiffs had produced evidence that Napster use harmed the markets for their copyrighted works by (i) reducing CD sales among college students and (ii) raising barriers to plaintiffs’ own entry into the market for digital downloading of music because of competition from a service from which recordings could be obtained free.²¹⁸² The Ninth Circuit affirmed all of these rulings in Napster I.²¹⁸³

4. The Sony Doctrine of Substantial Noninfringing Uses. Napster argued that it could not be contributorily or vicariously liable for operating the Napster service under the doctrine of Sony Corp. of Am. v. Universal City Studios, Inc.,²¹⁸⁴ which held that a manufacturer is not liable for contributory infringement for selling a staple article of commerce that is “capable of commercially significant noninfringing uses,”²¹⁸⁵ even if that article is used to commit copyright infringement. Napster raised a number of uses of the Napster system that it argued were both actual and potential commercially significant noninfringing uses. The district court found that the specific uses raised by Napster were in fact infringing:

5. Sampling. Napster argued that many users use Napster to sample unfamiliar music and then, if they like it, go purchase the music on CD. Napster argued that downloads initiated for sampling purposes and followed up by a purchase of the music, constituted fair use. The district court rejected this argument, ruling that sampling on Napster was not a “personal use in the traditional sense that courts have recognized – copying which occurs within the household and does not confer any financial benefit on the user,” and that instead sampling on Napster amounted to “obtaining permanent copies of songs that users would otherwise have to purchase; it also carries the potential for viral distribution to millions of people.”²¹⁸⁶ The court

²¹⁸¹ Napster, 114 F. Supp. 2d at 913.

²¹⁸² Id. Napster submitted survey evidence which it argued showed that Napster use actually stimulated more sales of CDs containing the plaintiffs’ works than it displaced. The court did not find this evidence credible, and instead credited evidence submitted by the plaintiffs’ experts which the plaintiffs claimed showed that Napster use was likely to reduce CD purchases by college students. Id. at 909-10.

²¹⁸³ Napster I., 239 F.3d at 1016-17.

²¹⁸⁴ 464 U.S. 417 (1984).

²¹⁸⁵ Id. at 442.

²¹⁸⁶ Napster, 114 F. Supp. 2d at 913. This language suggests that the court may have misunderstood Napster’s argument about sampling, for the court included under the “sampling” rubric instances in which users downloaded and retained a permanent copy of songs which they “would otherwise have to purchase.” Napster defined “sampling” to be those instances in which a user downloaded a song, then followed up with a purchase of the CD containing the song. In such instances, users would not be obtaining music that they “would otherwise have to purchase,” and Napster argued that such instances of true sampling should be deemed a fair use. In any event, the district court found not credible a survey submitted by Napster’s expert showing that 60% of online users who download free digital music do so to preview music before buying the CD, because Napster’s expert did not conduct the survey. The court further found a survey that the expert did conduct not to be credible because the court found it inadequately supervised by the expert. Id. at 914. Finally, the court

distinguished this kind of sampling activity from the time-shifting of viewing that the Supreme Court found a fair use in Sony, where time-shifting enabled a viewer to witness a broadcast that the viewer had been invited to view in its entirety free of charge; by contrast, the court noted that the plaintiffs almost always charged for their music. In addition, the court noted that the majority of VCR purchasers in Sony did not distribute taped television broadcasts, whereas a Napster user who downloads a copy of a song could make that song available to millions of other individuals.²¹⁸⁷ “The global scale of Napster usage and the fact that users avoid paying for songs that otherwise would not be free militates against a determination that sampling by Napster users constitute personal or home use in the traditional sense.”²¹⁸⁸

On appeal, Napster argued that the district court erred in concluding that sampling is a commercial use because it conflated a noncommercial use with a “personal use”; erred in determining that sampling adversely affects the market for plaintiffs’ copyrighted music; and erroneously concluded that sampling is not a fair use because it determined that samplers may also engage in other infringing activity.²¹⁸⁹ The Ninth Circuit in Napster I rejected these challenges, ruling that the plaintiffs had “established that they are likely to succeed in proving that even authorized temporary downloading of individual songs for sampling purposes is commercial in nature,” based on evidence in the record that the record company plaintiffs collect royalties for song samples available on Internet retail sites and that such samples, unlike in the case of Napster, are only partial samples of the whole work and often time out after download.²¹⁹⁰ In addition, the Ninth Circuit concluded that the record supported the district court’s preliminary determinations that the more music that sampling users download, the less likely they are to eventually purchase the recordings on CD, and even if the audio market is not harmed, Napster had adverse effects on the developing digital download market.²¹⁹¹ “[P]ositive impact in one market, here the audio CD market, [should not] deprive the copyright holder of the right to develop identified alternative markets, here the digital download market.”²¹⁹²

6. Space-Shifting. As an additional noninfringing use, Napster argued that many Napster users use the service to “space-shift,” i.e., “converting a CD the consumer already owns into MP3 format and using Napster to transfer the music to a different computer – from home to office, for example.”²¹⁹³ The district court found that such use was a de minimis portion of Napster use

ruled that even if sampling did enhance sales of plaintiffs’ CDs, that would not tip the balance in favor of fair use, because “courts have rejected the suggestion that a positive impact on sales negates the copyright holder’s entitlement to licensing fees or access to derivative markets.” Id.

²¹⁸⁷ Id. at 913.

²¹⁸⁸ Id. at 914.

²¹⁸⁹ Napster I, 239 F.3d at 1018.

²¹⁹⁰ Id.

²¹⁹¹ Id.

²¹⁹² Id.

²¹⁹³ Napster, 114 F. Supp. 2d at 904.

and not a significant aspect of Napster's business, and could therefore not qualify as a substantial noninfringing use under Sony:

According to the court's understanding of the Napster technology, a user who wanted to space-shift files from her home to her office would have to log-on to the system from her home computer, leave that computer online, commute to work, and log-on to Napster from her office computer to access the desired file. Common sense dictates that this use does not draw users to the system.²¹⁹⁴

As support for its argument that space-shifting constitutes a fair use, Napster invoked the passage, quoted in subsection 2 above, discussing the AHRA from the Ninth Circuit's decision in Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys.²¹⁹⁵ In particular, Napster focused on the last sentence of that passage, in which the Ninth Circuit stated, "The Rio merely makes copies in order to render portable, or 'space-shift,' those files that already reside on a user's hard drive."²¹⁹⁶ Napster argued that by virtue of this passage, the Ninth Circuit had held that space-shifting of works already owned constitutes a fair use.

The district court rejected this argument, ruling that Napster's reliance on the Diamond decision was erroneous because that was "a case involving an inapplicable statute [the AHRA]."²¹⁹⁷ The court also rejected any implication that space-shifting was sufficiently analogous to the time-shifting of television broadcasts that the Supreme Court found to be a substantial noninfringing use in Sony. In particular, the court ruled that in Sony, the Supreme Court had determined that time-shifting represented the principal, rather than an occasional use of VCRs, whereas Napster had failed to show that space-shifting constituted a "commercially significant" use of Napster. "Thus, even if space-shifting is a fair use, it is not substantial enough to preclude liability under the staple article of commerce doctrine."²¹⁹⁸

On appeal in Napster I, the Ninth Circuit agreed with the district court that the "shifting" analyses of both Sony and Diamond were inapposite because "the methods of shifting in these cases did not also simultaneously involve distribution of the copyrighted material to the general public; the time or space-shifting of copyrighted material exposed the material only to the original user."²¹⁹⁹

7. Authorized Distributions. Napster argued that many artists had authorized distributions of their works through the Napster system, and that such authorized uses constituted substantial noninfringing uses under Sony. Napster set up a "New Artist Program,"

²¹⁹⁴ Id. at 904-05.

²¹⁹⁵ 180 F.3d 1072 (9th Cir. 1999).

²¹⁹⁶ Id. 1079 (citations omitted).

²¹⁹⁷ Napster, 114 F. Supp. 2d at 915.

²¹⁹⁸ Id. at 916.

²¹⁹⁹ Napster I, 239 F.3d at 1019.

pursuant to which new or unsigned artists could promote their works and distribute them in MP3 format via the Napster service. Napster accepted enrollment of new artists in its program only if the artist explicitly authorized Napster users to share the artist's music.²²⁰⁰ The district court, however, held that "the New Artist Program may not represent a substantial or commercially significant aspect of Napster,"²²⁰¹ essentially ruling that it had been an afterthought: "[T]he court finds that the New Artist Program accounts for a small portion of Napster use and did not become central to defendant's business strategy until this action made it convenient to give the program top billing. An early version of the Napster website advertised the ease with which users could find their favorite popular music without 'wading through page after page of unknown artists.' Defendant did not even create the New Artist Program that runs on its Internet website until April 2000 – well after plaintiffs filed this action."²²⁰²

In any event, the court concluded that, because it believed the activity under the New Artist Program to be separable from the infringing activity of the unauthorized distribution of the plaintiffs' works, the New Artist Program was insufficient to save Napster under the Sony doctrine: "Napster's primary role of facilitating the unauthorized copying and distribution of established artists' songs renders *Sony* inapplicable. ... Because plaintiffs do not ask the court to shut down such satellite activities, the fact that these activities may be noninfringing does not lessen plaintiffs' likelihood of success."²²⁰³

In conclusion, the district court rejected applicability of the Sony doctrine on the ground that "any potential noninfringing use of the Napster service is minimal or connected to the infringing activity, or both. The substantial or commercially significant use of the services was, and continues to be, the unauthorized downloading and uploading of popular music, most of which is copyrighted."²²⁰⁴

On appeal in Napster I, the Ninth Circuit disagreed with the district court's overall conclusion that the Napster system was incapable of substantial noninfringing uses: "The district court improperly confined the use analysis to current uses, ignoring the system's capabilities. ... Consequently, the district court placed undue weight on the proportion of current infringing uses as compared to current and future noninfringing use."²²⁰⁵ The Ninth Circuit therefore

²²⁰⁰ Napster, 114 F. Supp. 2d at 907.

²²⁰¹ Id. at 917. It is unclear why the court used the term "may," since that leaves open the possibility that the New Artist Program might constitute a substantial or commercially significant aspect of Napster, which in turn would affect the analysis under the Sony doctrine.

²²⁰² Id. at 904 (citations omitted). One of plaintiffs' experts submitted results of a sample of 1150 files on the Napster service, in which were contained only 11 new artists and 14 of their music files. Id.

²²⁰³ Id. at 917. On appeal, the Ninth Circuit, with no further analysis, simply noted that the plaintiffs had not requested that Napster's New Artist Program be enjoined. Napster I, 239 F.3d at 1019.

²²⁰⁴ Napster, 114 F. Supp. 2d at 912.

²²⁰⁵ Napster I, 239 F.3d at 1021.

concluded that the Napster system was in fact capable of substantial noninfringing uses.²²⁰⁶ Nevertheless, for the reasons set forth in the next subsection, that conclusion was not sufficient to save Napster from liability under the Sony doctrine.

8. Ongoing Control by Napster Over Its Service. In addition to rejecting all of Napster's arguments of noninfringing uses of its system, the district court ruled that the Sony doctrine was inapplicable to Napster for one final reason – because Napster exercised ongoing control over its service (which was the same control that the court concluded provided a basis in part for its finding of both contributory and vicarious liability, as analyzed below). The plaintiffs had argued that the Sony doctrine was applicable only to the manufacture and sale of an article of commerce, and not to a service. Although the district court appears not to have accepted this device/service distinction per se, the district court did note that in Sony, the defendant's participation did not extend past the manufacturing and selling of the VCRs, and the defendant had no ongoing participation in the use of the devices to commit infringing acts.²²⁰⁷

Courts have distinguished the protection *Sony* offers to the manufacture and sale of a device from scenarios in which the defendant continues to exercise control over the device's use. ... Given defendant's control over the service, as opposed to mere manufacturing or selling, the existence of a potentially unobjectionable use like space-shifting does not defeat plaintiffs' claims.²²⁰⁸

On appeal, the Ninth Circuit in Napster I also did not draw a distinction between a device and a service for purposes of applying the Sony doctrine, but rather, like the district court, distinguished between the Napster service itself and Napster's relation to the operational use of the system: "We are compelled to make a clear distinction between the architecture of the Napster system and Napster's conduct in relation to the operational capacity of the system."²²⁰⁹ Thus, Napster could not be contributorily liable merely for offering a service that could be used for infringing uses, but could be liable if it had sufficient specific knowledge of use of the service for infringing purposes in particular instances.²²¹⁰ This knowledge requirement is discussed further in the next subsection.

9. The Elements of Contributory Liability. In order to establish contributory liability for the acts of direct infringement by Napster's users, the district court noted that the plaintiffs

²²⁰⁶ Id.

²²⁰⁷ Napster, 114 F. Supp. 2d at 916-17.

²²⁰⁸ Id. at 917 (citations omitted).

²²⁰⁹ Napster I, 239 F.3d at 1020.

²²¹⁰ Id. at 1020-21.

were required to show that Napster had knowledge of the infringing activity and that it induced, caused or materially contributed to the infringing conduct.²²¹¹

(i) The Knowledge Prong. With respect to the knowledge prong, the district court found the plaintiffs had presented convincing evidence that Napster had both actual and constructive knowledge of its users' infringements. The district court found actual knowledge because: (1) a document authored by a co-founder of Napster, Sean Parker, mentioned the need to remain ignorant of users' real names and IP addresses "since they are exchanging *pirated* music";²²¹² and (2) the RIAA had informed Napster of more than 12,000 infringing music files being shared through the Napster system.²²¹³ Although Napster had terminated the accounts of the users offering those files, the district court noted that the songs were still available using the Napster service, as were other copyrighted works identified in the Schedules to the plaintiffs' complaint.²²¹⁴ The district court found constructive knowledge on Napster's part because: (1) Napster executives had recording industry experience; (2) Napster possessed enough sophistication about intellectual property laws to make claims against a rock band that copied its logo; (3) Napster executives had downloaded copyrighted songs from the system; and (4) they had promoted the site with screen shots listing infringing files.²²¹⁵

Napster had argued that the law of contributory infringement requires actual knowledge of specific acts of infringement (which Napster argued that it did not have),²²¹⁶ that mere generalized knowledge that the Napster system might be used for infringing transmissions was not sufficient for contributory liability, and that in every instance in which Napster received actual knowledge from the plaintiffs of infringing acts by a specific user, Napster had acted to terminate such infringing activity. The district court rejected this argument, ruling that actual knowledge of specific acts of infringement is not required for contributory liability, citing Gershwin Publ'g Corp. v. Columbia Artists Management, Inc.,²²¹⁷ which the court characterized as holding that general knowledge that third parties performed copyrighted works satisfied the knowledge element of contributory infringement. Accordingly, "the court rejects defendant's

²²¹¹ Napster, 114 F. Supp. 2d at 918 (citing Gershwin Publ'g Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)).

²²¹² 114 F. Supp. 2d at 918 (emphasis in original).

²²¹³ Id.

²²¹⁴ Id.

²²¹⁵ Id. at 919.

²²¹⁶ Napster argued that it had no specific knowledge that any particular use of a file through its system was unauthorized. In particular, Napster argued that it could not know, any more than a photocopier or video recorder manufacturer, which uses of its system were fair or not. Napster further argued that it could not know the copyright status of its users' files. Neither CD audio files nor the resultant MP3 files carried any copyright notice or watermark. MP3 file names are created by users, contain errors, and are variable and undependable. Finally, Napster argued that song titles could not be used to distinguish authorized files from others because many song titles are used by multiple artists or there may be multiple recordings of the same work – some of which are authorized to be shared and others not. Napster's Pl. Opp. Br., supra note 2163, at 18-19.

²²¹⁷ 443 F.2d 1159, 1163 (2d Cir. 1971).

argument that titles in the Napster directory cannot be used to distinguish infringing from noninfringing files and thus that defendant cannot know about infringement by any particular user of any particular musical recording or composition.”²²¹⁸

The district court also rejected Napster’s reliance on the following passage from the Netcom decision concerning contributory liability of service providers:

Where a BBS [bulletin board service] operator cannot reasonably verify a claim of infringement, either because of a possible fair use defense, the lack of copyright notices on the copies, or the copyright holder’s failure to provide the necessary documentation to show that there is likely infringement, the operator’s lack of knowledge will be found reasonable and there will be no liability for contributory infringement for allowing the continued distribution of the works on its system.²²¹⁹

The district court held that this language was dicta because the plaintiffs in that case raised a genuine issue of material fact regarding knowledge. But more importantly, the court ruled that Napster “is not an Internet service provider that acts as a mere conduit for the transfer of files.”²²²⁰

One of the important issues on appeal was whether constructive knowledge is sufficient for contributory liability, or whether actual knowledge of infringing uses is required for liability. The Ninth Circuit in Napster I began its analysis of the knowledge prong by stating that contributory liability “requires that the secondary infringer ‘know or have reason to know’ of direct infringement.”²²²¹ The Ninth Circuit also stated, “It is apparent from the record that Napster has knowledge, both actual and constructive, of direct infringement.”²²²² Both of these statements suggest that constructive knowledge is sufficient to impose contributory liability on a service provider.

However, further analysis by the Ninth Circuit in its Napster I opinion suggests that constructive knowledge in the general sense that a service provider may know that its system could potentially be used for infringing purposes, is insufficient. Specifically, the Ninth Circuit stated, “We are bound to follow Sony, and will not impute the requisite level of knowledge to Napster merely because peer-to-peer file sharing technology may be used to infringe plaintiffs’ copyrights.”²²²³ Nevertheless, the Ninth Circuit found that “the evidentiary record here

²²¹⁸ Napster, 114 F. Supp. 2d at 918.

²²¹⁹ Religious Technology Center v. Netcom Online Communication Services, Inc., 907 F. Supp. 1361, 1374 (N.D. Cal. 1995).

²²²⁰ Napster, 114 F. Supp. 2d at 919.

²²²¹ Napster I, 239 F.3d at 1020 (citing Cable/Home Communication Corp. v. Network Prods., Inc., 902 F.2d 829, 845 & 846 n.29 (11th Cir. 1990)).

²²²² Napster I, 239 F.3d at 1020.

²²²³ Id. at 1020-21.

supported the district court’s finding that plaintiffs would likely prevail in establishing that Napster knew or had reason to know of its users’ infringement of plaintiffs’ copyrights.”²²²⁴

The Ninth Circuit endorsed the analysis of the Netcom decision, “which suggests that in an online context, evidence of actual knowledge of specific acts of infringement is required to hold a computer system operator liable for contributory copyright infringement.”²²²⁵ The reference to “actual knowledge” raises the question whether the Ninth Circuit meant to exclude constructive knowledge as being sufficient. However, the Ninth Circuit went on to state that the “court [in Netcom] determined that for the operator to have sufficient knowledge, the copyright holder must ‘provide the necessary documentation to show there is likely infringement.’”²²²⁶ From this statement, it appears that specific notice from the copyright holder of activity on the service sufficient to show that there is “likely” infringement can constitute “reason to know.” Thus, the form of constructive knowledge the Ninth Circuit in Napster I appears to contemplate as giving rise to potential liability is only one that flows from very specific notice by a copyright holder of particular potentially infringing activity on the service. What is unclear, however, as further analyzed below, is the extent to which, once a service provider has been notified of a particular infringing instance of a work on the service, the service provider then has “constructive knowledge” of the presence of that work on its service that gives rise to a duty to police for other infringing occurrences of that work on the system.

Summarizing its endorsement of the Netcom approach, the Ninth Circuit ruled in Napster I that “if a computer system operator learns of specific infringing material on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement. Conversely, absent any specific information which identifies infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material.”²²²⁷ The Ninth Circuit concluded that the record established sufficient knowledge to impose contributory liability on Napster “when linked to demonstrated infringing use of the Napster system. The record supports the district court’s finding that Napster has actual knowledge that specific infringing material is available using its system, that it could block access to the system by suppliers of the infringing material, and that it failed to remove the material.”²²²⁸ Again, the Ninth Circuit’s

²²²⁴ Id. at 1021.

²²²⁵ Id. (citing Religious Technology Center v. Netcom On-Line Communications Servs., 907 F. Supp. 1361, 1371 (N.D. Cal. 1995)).

²²²⁶ Napster I, 239 F.3d at 1021 (quoting Netcom, 907 F. Supp. at 1374).

²²²⁷ Napster I, 239 F.3d at 1021 (citations omitted).

²²²⁸ Id. at 1022 (citations omitted; emphasis in original). The second element in the second sentence – that Napster could block access to the system by suppliers of infringing material – hints of a requirement of “control” over the infringing activity in the contributory liability analysis. As analyzed below with respect to the imposition of vicarious liability on Napster, a “control” test has generally been relevant only to vicarious liability. It is unclear whether the Ninth Circuit really meant to introduce a new “control” test into contributory liability.

reference to “actual” knowledge raises confusion about the extent to which constructive knowledge can give rise to contributory liability.

(ii) The Material Contribution Prong. With respect to the material contribution prong of the contributory liability test, the district court ruled that Napster had materially contributed to the infringing acts of its users. For support, the court cited Fonovisa, Inc. v. Cherry Auction, Inc.,²²²⁹ in which the owners of copyrights for musical recordings stated a contributory infringement claim against the operators of a swap meet at which independent vendors sold counterfeit recordings, because it would have been difficult for the infringing activity to take place in the massive quantities alleged without the support services provided by the swap meet. The district court found that Napster was essentially an Internet swap meet and that Napster was materially contributing to the infringing activity of its users by supplying the MusicShare software, search engine, servers, and means of establishing a connection between users’ computers.²²³⁰ “Without the support services defendant provides, Napster users could not find and download the music they want with the ease of which defendant boasts.”²²³¹

On appeal in Napster I, the Ninth Circuit found that the district court had correctly applied the reasoning of Fonovisa. “We agree that Napster provides ‘the site and facilities’ for direct infringement.”²²³² The Ninth Circuit’s view of the material contribution prong appears to be very broad sweeping, for it would seem that all service providers provide “the site and facilities” for any direct infringement that may occur on the service. If this is the only test for material contribution, it may be difficult for a service provider to use the material contribution prong as a defense to common law contributory liability.

10. The Elements of Vicarious Liability and the Duty to Police.²²³³ In order to establish vicarious liability for the acts of direct infringement by Napster’s users, the district court noted that the plaintiffs were required to show that Napster had the right and ability to supervise the infringing activity of its users and had a direct financial interest in such activity.²²³⁴ Napster argued that it did not have the ability to supervise the allegedly infringing activity because it was impossible to police the activity of each of its individual users. Napster argued that it could never know the use to which a particular file was put on its system, and thus could not control

²²²⁹ 76 F.3d 259 (9th Cir. 1996).

²²³⁰ Napster, 114 F. Supp. 2d at 919-20.

²²³¹ Id. at 920.

²²³² Napster I, 239 F.3d at 1022.

²²³³ Although the issue of online vicarious liability is treated generally in Section III.C.3 below, the vicarious liability issues in the Napster case will be treated here in order, for clarity, to present the entire analysis of secondary liability issues involved in the case in a single place.

²²³⁴ Napster, 114 F. Supp. 2d at 920.

whether a use was fair or not. Napster also pointed to Section 512(m) of the DMCA,²²³⁵ which provides that a service provider has no affirmative duty to police its users, and cannot be expected to monitor individual users until put on notice by the copyright holder of particular alleged infringing materials. Napster argued that, were service providers required affirmatively to identify and exclude all copyrighted materials, there could be no file sharing or, indeed, even a World Wide Web.²²³⁶ Napster also argued that it received no direct financial benefit from the infringing activity, but at most only a generalized financial benefit, since the many noninfringing uses of the Napster system drew many users to its system.²²³⁷

The district court rejected these arguments and ruled that Napster was vicariously liable. The court found that Napster's ability to block users about whom rights holders complain was "tantamount to an admission that defendant can, and sometimes does, police its service."²²³⁸ The court ruled that a defendant need not exercise its supervisory powers to be deemed capable of doing so. The district court also held that the plaintiffs had shown a reasonable likelihood that Napster had a direct financial interest in the infringing activity, citing documents stating that Napster would derive revenues directly from increases in its user base and deposition testimony by Napster's former President that the Napster service attracted more and more users by offering an increasing amount of quality music for free. The court found this to be similar to the type of direct financial interest that the Ninth Circuit found sufficient for vicarious liability in the Fonovisa case. Accordingly, the district court ruled that the plaintiffs had shown a reasonable likelihood of success on their vicarious infringement claims.²²³⁹

The Ninth Circuit's rulings on appeal in Napster I with respect to the vicarious liability issue are some of the most significant holdings in the case. In a very important initial ruling, the Ninth Circuit held that the "staple article of commerce" doctrine of Sony has *no* applicability to vicarious liability. This ruling seems a bit odd, since the Sony opinion uses the phrase "vicarious liability" several times. The Ninth Circuit acknowledged as much, but concluded that "when the Sony Court used the term 'vicarious liability,' it did so broadly and outside of a technical analysis of the doctrine of vicarious copyright infringement." Under this holding, it appears that the Sony doctrine will not afford any immunity to service providers from vicarious liability.

The Ninth Circuit's view of the vicarious liability doctrine was broad on both the financial benefit and supervision prongs. With respect to the financial benefit prong, the Ninth Circuit, citing Fonovisa, agreed with the district court that "financial benefit exists where the availability

²²³⁵ That section provides as follows: "Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) [the safe harbors] on – (1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i)." 17 U.S.C. § 512(m)(1).

²²³⁶ Napster's PI Opp. Brief, supra note 2163, at 20-21.

²²³⁷ Id. at 21.

²²³⁸ Napster, 114 F. Supp. 2d at 921.

²²³⁹ Id. at 921-22.

of infringing material ‘acts as a “draw” for customers.’”²²⁴⁰ The Ninth Circuit relied on the district court’s finding that more users register with the Napster system as the quality and quantity of available music increases.²²⁴¹

With respect to the supervision prong, the Ninth Circuit noted that “Napster has an express reservation of rights policy, stating on its website that it expressly reserves the ‘right to refuse service and terminate accounts in [its] discretion, including, but not limited to, if Napster believes that user conduct violates applicable law ... or for any reason in Napster’s sole discretion, with or without cause.’”²²⁴² The Ninth Circuit ruled that this reservation of rights policy was, of itself, sufficient evidence of Napster’s right and ability to supervise its users’ conduct, and (in one of the most important aspects of the entire opinion), gave rise to a *duty to police* the Napster system: “To escape imposition of vicarious liability, the reserved right to police must be exercised to its fullest extent. Turning a blind eye to detectable acts of infringement for the sake of profit gives rise to liability.”²²⁴³

This holding raises a number of significant issues. First, the ruling that a reservation of rights policy by itself satisfies the supervision prong of the vicarious liability test puts service providers in a potential Catch 22 situation with the DMCA. As discussed further below, under Section 512(i) of the DMCA, in order to be eligible for the safe harbors of the DMCA, a service provider must adopt and reasonably implement a “policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider’s system or network who are repeat infringers.” Under the Ninth Circuit’s ruling in Napster I, however, the adoption of such a policy would seem to expose the service provider to vicarious liability under the supervision prong. The service provider is therefore put in a Catch 22 – whether it should avoid adoption of a reservation of rights policy in order to avoid common law liability, thereby potentially giving up its DMCA safe harbors, or preserve its DMCA safe harbors by adopting such a policy, thereby potentially increasing its exposure to vicarious liability.

Second, the duty to police seems contrary to Section 512(m) of the DMCA, which states that a service provider need not “monitor[] its service or affirmatively seek[] facts indicating infringing activity, except to the extent consistent with a standard technical measure” in order to be eligible for the DMCA safe harbors. Thus, the Ninth Circuit’s opinion in Napster I seems to require that a service provider do more than is required by the DMCA in order to avoid common law secondary liability.

Third, the Ninth Circuit did not specifically define what constitutes a “detectable” act of infringement, and the scope of the duty to police for such acts is therefore unclear under its opinion. The Ninth Circuit noted, however, that the district court’s original injunction (discussed

²²⁴⁰ Napster I, 239 F.3d at 1023 (quoting Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 263-64 (9th Cir. 1996)).

²²⁴¹ Napster I, 239 F.3d at 1023.

²²⁴² Id.

²²⁴³ Id.

in detail in subsection 13 below) had gone too far in what it required Napster to do. The district court's original injunction ruled that "Napster bears the burden of developing a means to comply with the injunction," which would have required Napster to develop new blocking technology that did not exist in its system. The preliminary injunction further required that Napster "must insure that no work owned by plaintiffs which neither defendant nor Napster users have permission to use or distribute is uploaded or downloaded on Napster."

The Ninth Circuit ruled in Napster I that this preliminary injunction went too far in the burden it placed on Napster to police. Analogizing to the Fonovisa case, which imposed secondary liability on the operator of the swap meet because the operator had the right and ability to police the premises of the swap meet, the Ninth Circuit ruled that the district court "failed to recognize that the boundaries of the premises that Napster 'controls and patrols' are limited. ... Put differently, Napster's reserved 'right and ability' to police is cabined by the system's current architecture. As shown by the record, the Napster system does not 'read' the content of indexed files, other than to check that they are in the proper MP3 format."²²⁴⁴ The Ninth Circuit went on to rule that Napster's duty to police must be limited by the existing architecture of its system:

Napster, however, has the ability to locate infringing material listed on its search indices, and the right to terminate users' access to the system. The file name indices, therefore, are within the "premises" that Napster has the ability to police. We recognize that the files are user-named and may not match copyrighted material exactly (for example, the artist or song could be spelled wrong). For Napster to function effectively, however, file names must reasonably or roughly correspond to the material contained in the files, otherwise no user could ever locate any desired music. As a practical matter, Napster, its users and the record company plaintiffs have equal access to infringing material by employing Napster's "search function."²²⁴⁵

This passage suggests that Napster's obligations to police its system for infringing files was to be limited to monitoring the names of files made available for sharing by Napster users using the existing search function of the Napster system, which the Ninth Circuit noted was equally available to both the plaintiffs and Napster for policing for infringing files. Unlike the district court's original preliminary injunction, then, the Ninth Circuit in Napster I did not contemplate that Napster would be required to develop new technology for policing not based on file name searches (such as digital "fingerprinting" of the content of files or other techniques).

11. Summary of Secondary Liability Under the Ninth Circuit's Decision. At the end of its opinion in Napster I, the Ninth Circuit offered the following summary of its standard for contributory liability and vicarious liability:

²²⁴⁴ Id. at 1023-24.

²²⁴⁵ Id. at 1024.

[C]ontributory liability may potentially be imposed only to the extent that Napster: (1) receives reasonable knowledge of specific infringing files with copyrighted musical compositions and sound recordings; (2) knows or should know that such files are available on the Napster system; and (3) fails to act to prevent viral distribution of the works. The mere existence of the Napster system, absent actual notice and Napster's demonstrated failure to remove the offending material, is insufficient to impose contributory liability.

Conversely, Napster may be vicariously liable when it fails to affirmatively use its ability to patrol its system and preclude access to potentially infringing files listed in its search index. Napster has both the ability to use its search function to identify infringing musical recordings and the right to bar participation of users who engage in the transmission of infringing files.²²⁴⁶

This summary replicates many of the ambiguities noted earlier with respect to (i) whether constructive knowledge is sufficient for liability (the summary first speaks of "knowledge of specific infringing files" but then speaks of whether Napster "should know" that such files are available on its system) and (ii) the scope of the duty to police (the summary speaks of blocking access to "potentially" infringing files without defining when a file is "potentially" infringing, and of preventing "viral distribution" of "works," without saying whether, by use of the term "works," it meant to reference only particular files of which Napster has notice, or any files that may contain the copyrighted "work").

12. Other Defenses Raised by Napster Rejected by the District Court and the Ninth Circuit.²²⁴⁷ The court also rejected a number of other miscellaneous defenses to liability that Napster had raised, which may be summarized briefly as follows:

(i) First Amendment. Napster argued that the requested injunction would impose an overbroad prior restraint on its free speech rights to publish a directory of where files were located on its users' computers, as well as that of its users and the unsigned artists who depend on the Napster service to gain exposure by distributing their music through Napster. The district court rejected this argument, finding that free speech concerns "are protected by and coextensive with the fair use doctrine."²²⁴⁸ The parties sharply disputed the extent to which infringing and noninfringing aspects of the Napster service were separable, and whether it was therefore practical for the court to enjoin only the infringing aspects. The district court ruled, however, that even if it were "technologically impossible for Napster, Inc. to offer such functions as its directory without facilitating infringement, the court still must take action to protect

²²⁴⁶ Id. at 1027 (citations omitted).

²²⁴⁷ Napster also raised defenses under the safe harbors of the DMCA, which are discussed in Section III.C.6(b) below.

²²⁴⁸ Napster, 114 F. Supp. 2d at 922 (citing Nihon Keizai Shimbun, Inc. v. Comline Bus. Data, Inc., 166 F.3d 65, 74 (2d Cir. 1999)).

plaintiffs' copyrights."²²⁴⁹ On appeal in Napster I, the Ninth Circuit, in a very terse analysis of the First Amendment issue, simply ruled that "First Amendment concerns in copyright are allayed by the presence of the fair use doctrine. ... Uses of copyrighted material that are not fair uses are rightfully enjoined."²²⁵⁰

(ii) Copyright Misuse. Napster argued that the plaintiff record labels were engaged in copyright misuse by attempting to aggrandize their monopoly beyond the scope of their copyrights by restricting the flow of unsigned artists' music, which competed with their own, and by controlling the distribution of music over the Internet. The district court rejected this argument, concluding that most of the copyright misuse cases involved the attempt to enlarge a copyright monopoly through restricted or exclusive licensing, and the plaintiffs in the instant case had granted no licenses to Napster, let alone impermissibly restrictive ones.²²⁵¹ On appeal in Napster I, the Ninth Circuit affirmed the ruling of the district court, finding no evidence that the plaintiffs sought to control areas outside their grant of monopoly. "Rather, plaintiffs seek to control reproduction and distribution of their copyrighted works, exclusive rights of copyright holders."²²⁵² In a footnote, however, the Ninth Circuit did note that the copyright misuse doctrine is not limited entirely to situations of restrictive licensing – "a unilateral refusal to license a copyright may constitute wrongful exclusionary conduct giving rise to a claim of misuse, but [we] assume that the 'desire to exclude others ... is a presumptively valid business justification for any immediate harm to consumers."²²⁵³

(iii) Waiver. Napster asserted that the plaintiffs had waived their right to enforce their copyrights against Napster. Napster introduced evidence that the plaintiffs had known of the existence of "ripping" software for creating MP3 files for years, and had known that making MP3 files from CDs was the most prevalent means by which sound recordings became available for transfer over the Internet in the first place, yet had failed to take any actions to stop or even slow its widespread proliferation, and indeed had actively formed partnerships with and invested in companies that directed consumers to MP3 encoding software that would enable them to transfer music files over the Internet.²²⁵⁴ The district court responded as follows:

This limited evidence fails to convince the court that the record companies created the monster that is now devouring their intellectual property rights. Although plaintiffs have not sued their business partners for contributory infringement, they typically have asked them to discourage unauthorized ripping and have made security part of their agreements. Defendant fails to show that, in hastening the proliferation of MP3 files,

²²⁴⁹ Napster, 114 F. Supp. 2d at 923.

²²⁵⁰ Napster I, 239 F.3d at 1028.

²²⁵¹ Napster, 114 F. Supp. 2d at 923.

²²⁵² Napster I, 239 F.3d at 1027.

²²⁵³ *Id.* at 1027 n.8 (citing Image Tech. Servs. V. Eastman Kodak Co., 125 F.3d 1195, 1218 (9th Cir. 1997)).

²²⁵⁴ Napster's PI Opp. brief, *supra* note 2163, at 22.

plaintiffs did more than seek partners for their commercial downloading ventures and develop music players for files they planned to sell over the Internet.²²⁵⁵

On appeal in Napster I, the Ninth Circuit affirmed this ruling, citing the district court's finding that "in hastening the proliferation of MP3 files, plaintiffs did [nothing] more than seek partners for their commercial downloading ventures and develop music players for files they planned to sell over the Internet."²²⁵⁶

(iv) Failure to Present Evidence of Copyright Registration. Finally, Napster argued that, under section 411(a) of the copyright statute,²²⁵⁷ in order to claim infringement of multiple works, the plaintiffs were required to specify the works with particularity and provide proof of copyright registration for those works. Napster noted that the plaintiffs had identified only a discrete number of works allegedly infringed, together with their registration numbers, in a Schedule to their complaint, and argued that the plaintiffs had no jurisdiction to assert the copyrights in other unidentified works. The court rejected this argument, citing a 1990 case from the D.C. Circuit as authority for the proposition that a court may enter an injunction in a copyright case covering works owned by the plaintiff but not in suit, particularly where there has been a history of continuing infringement and there exists a significant threat of future infringement.²²⁵⁸

On appeal in Napster I, the Ninth Circuit failed to address this argument directly. Instead, it simply ruled that the plaintiffs had sufficiently demonstrated "ownership" for purposes of a prima facie case of direct infringement, quoting the district court's statement that "as much as eighty-seven percent of the files available on Napster may be copyrighted and more than seventy percent may be owned or administered by plaintiffs."²²⁵⁹

13. The Mar. 5, 2001 Preliminary Injunction. The district court ruled that, because the plaintiffs had shown a reasonable likelihood of success on the merits of their contributory and vicarious²²⁶⁰ copyright infringement claims, they were entitled to a presumption of irreparable harm, and a preliminary injunction should issue. The district court therefore enjoined Napster "from engaging in, or facilitating others in copying, downloading, uploading, transmitting, or distributing plaintiffs' copyrighted musical compositions and sound recordings, protected by

²²⁵⁵ Napster, 114 F. Supp. 2d at 924.

²²⁵⁶ Napster I, 239 F.3d at 1026.

²²⁵⁷ That section provides that "no action for infringement of the copyright in any work shall be instituted until registration of the copyright claim has been made in accordance with this title." 17 U.S.C. §411(a).

²²⁵⁸ Napster, 114 F. Supp. 2d at 925 (citing Walt Disney Co. v. Powell, 897 F.2d 565, 568 (D.C. Cir. 1990)).

²²⁵⁹ Napster I, 239 F.3d at 1013 (quoting Napster, 114 F. Supp. 2d at 911) (emphasis added). It is puzzling why a showing that a certain percentage of the works on Napster "may" be copyrighted and "may" be owned by plaintiffs is sufficient to meet the very specific jurisdictional requirements of 17 U.S.C. § 411(a).

²²⁶⁰ The court's rationale for its rejection of Napster's defense under the safe harbors of the DMCA is discussed in Section III.C.6 below.

either federal or state law, without express permission of the rights owner.”²²⁶¹ The court further noted that “[b]ecause defendant has contributed to illegal copying on a scale that is without precedent, it bears the burden of developing a means to comply with the injunction. Defendant must insure that no work owned by plaintiffs which neither defendant nor Napster users have permission to use or distribute is uploaded or downloaded on Napster. The court ORDERS plaintiffs to cooperate with defendant in identifying the works to which they own copyrights.”²²⁶²

On July 28, 2000 (the day the district court had set for the preliminary injunction to go into effect), the Ninth Circuit issued a stay of the injunction, noting that the case “raised substantial questions of first impression going to both the merits and the form of the injunction.”²²⁶³ As discussed above, the Ninth Circuit ultimately ruled in Napster I that the district court’s original preliminary injunction was overbroad, and remanded the case for entry of a narrower preliminary injunction consistent with the Ninth Circuit’s opinion. Napster subsequently filed a petition with the Ninth Circuit for rehearing *en banc*, which was denied by order dated June 22, 2001.

On remand, both the plaintiffs and Napster each submitted proposed preliminary injunctions. On March 5, 2001, the district court entered a revised, narrower preliminary injunction requiring the plaintiffs to give notice to Napster of specific infringing file names on the Napster system and requiring Napster to block access to those file names through its search index, as well as reasonable variants of such file names that the parties might generate. The modified preliminary injunction required use of Napster’s file name search function as the centerpiece of Napster’s duty to police. The district court also permitted the record company plaintiffs to submit notices to Napster of new sound recordings in advance of their release, and required Napster to make efforts to do prophylactic blocking of such new recordings. Specifically, the revised preliminary injunction provided as follows in pertinent part:²²⁶⁴

“Plaintiffs shall provide notice to Napster of their copyrighted sound recordings by providing for each work:

- (A) the title of the work;
- (B) the name of the featured recording artist performing the work (“artist name”);
- (C) the name(s) of one or more files available on the Napster system containing such work; and
- (D) a certification that plaintiffs own or control the rights allegedly infringed.

²²⁶¹ Napster, 114 F. Supp. 2d at 927.

²²⁶² Id. The court ordered the plaintiffs to post a bond in the amount of \$5 million – far below what Napster had requested – to compensate Napster for losses in the event that the injunction was reversed or vacated. Id.

²²⁶³ Order, A&M Records, Inc. v. Napster, Inc., No. 00-16401, 2000 U.S. App. LEXIS 18688 (9th Cir. July 28, 2000).

²²⁶⁴ The text of the complete preliminary injunction may be found at 2001 U.S. Dist. LEXIS 2186 (N.D. Cal. Mar. 5, 2001).

Plaintiffs shall make a substantial effort to identify the infringing files as well as the names of the artist and title of the copyrighted recording.”²²⁶⁵

“All parties shall use reasonable measures in identifying variations of the filename(s), or of the spelling of the titles or artists’ names, of the works identified by plaintiffs. If it is reasonable to believe that a file available on the Napster system is a variation of a particular work or file identified by plaintiffs, all parties have an obligation to ascertain the actual identity (title and artist name) of the work and to take appropriate action within the context of this Order.”²²⁶⁶

“The Ninth Circuit held that the burden of ensuring that no copying, downloading, uploading, transmitting or distributing of plaintiffs’ copyrighted works occurs on the system is shared between the parties. The court ‘place[d] the burden on plaintiffs to provide notice to Napster’ and imposed on Napster the burden ‘of policing the system within the limits of the system.’ It appears to the court on the basis of the factual representations by the parties at the March 2, 2001 hearing that it would be difficult for plaintiffs to identify all infringing files on the Napster system given the transitory nature of its operation. This difficulty, however, does not relieve Napster of its duty. The court anticipates that it may be easier for Napster to search the files available on its system at any particular time against lists of copyrighted recordings provided by plaintiffs. The court deems that the results of such a search provide Napster with ‘reasonable knowledge of specific infringing files’ as required by the Ninth Circuit.”²²⁶⁷

“Once Napster ‘receives reasonable knowledge’ from any sources identified in preceding Paragraphs ... of specific infringing files containing copyrighted sound recordings, Napster shall, within three (3) business days, prevent such files from being included in the Napster index (thereby preventing access to the files corresponding to such names through the Napster system).”²²⁶⁸

“Within three (3) business days of receipt of reasonable notice of infringing files, Napster shall affirmatively search the names of all files being made available by all users at the time those users log on (i.e., prior to the names of files being included in the Napster index) and prevent the downloading, uploading, transmitting or distributing of the noticed copyrighted sound recordings.”²²⁶⁹

²²⁶⁵ Id. ¶ 2.

²²⁶⁶ Id. ¶ 3.

²²⁶⁷ Id. ¶ 4 (citations omitted).

²²⁶⁸ Id. ¶ 5.

²²⁶⁹ Id. ¶ 6. It is unclear what the difference is between the requirements of this paragraph and that of the previous paragraph. The district court may not have fully understood that the steps recited in this paragraph would be the same steps that Napster would take to comply with the previous paragraph.

“Plaintiffs may provide to Napster in advance of release the artist name, title of the recording, and release date of sound recordings for which, based on a review of that artist’s previous work, including but not limited to popularity and frequency of appearance on the Napster system, there is a substantial likelihood of infringement on the Napster system. Napster shall beginning with the first infringing file block access to or through its system to the identified recording. As Napster presently has the capability (even without enhancing its technology) to store information about and subsequently screen for a particular recording, the burden is far less and the equities are more fair to require Napster to block the transmission of these works in advance of their release. To order otherwise would allow Napster users a free ride for the length of time it would take plaintiffs to identify a specific infringing file and Napster to screen the work.”²²⁷⁰

Napster appealed, and the plaintiffs cross-appealed, the Mar. 5 modified preliminary injunction of the district court.

14. The Apr. 26, 2001 Clarification of the Preliminary Injunction. Many disputes between the plaintiffs and Napster quickly arose over the meaning and obligations imposed on the parties by the Mar. 5 modified injunction. First, the parties disputed whether the plaintiffs were required to provide notice to Napster of the names of specific files available on the Napster system containing the plaintiffs’ copyrighted sound recordings.²²⁷¹ The plaintiffs argued that the Ninth Circuit’s decision in Napster I required them to provide specific filenames only in support of their claims for contributory infringement, and not in support of their claims for vicarious liability, based on the following passage from Napster I:

The preliminary injunction we stayed is overbroad because it places on Napster the entire burden of ensuring that no “copying, downloading, uploading, transmitting, or distributing” of plaintiffs’ works occur on the system. As stated, we placed the burden on plaintiffs to provide notice to Napster of copyrighted works and files containing such works available on the Napster system before Napster has the duty to disable access to the offending content. Napster, however, also bears the burden of policing the system within the limits of the system. Here, we recognize that this is not an exact science in that the files are user named. In crafting the injunction on remand, the district court should recognize that Napster’s system does not currently appear to allow Napster access to users’ MP3 files.²²⁷²

The plaintiffs read this passage in two parts: First, they read that portion placing the “burden on plaintiffs to provide notice to Napster ... before Napster has the duty to disable access to the offending content,” as relating only to claims for contributory infringement; and second, that portion imposing on Napster the “burden of policing the system within the limits of the system,” as relating only to claims of vicarious infringement. Plaintiffs therefore maintained

²²⁷⁰ Id. ¶ 7.

²²⁷¹ Memorandum, In re Napster, Inc. Copyright Litigation, MDL No. C 00-1369 MHP (N.D. Cal. Apr. 26, 2001), at 1.

²²⁷² Id. at 1-2 (quoting Napster I, 239 F.3d at 1027).

that they were required to provide specific file names only to obtain preliminary relief on their claims of contributory infringement, but did not need to provide filenames to obtain preliminary relief on their claims of vicarious infringement.²²⁷³ The district court, although noting that the plaintiffs' reading of the paragraph might be "a prescient reading," nevertheless rejected it because the plain language of the paragraph did not allow for two separate standards, but rather "only one with several elements."²²⁷⁴

The parties also disputed whether the provision of the Mar. 5 modified injunction regarding the availability of the plaintiffs' copyrighted works prior to the official release of those works adequately resolved the plaintiffs' concerns. To aid its resolution of this issue, the court requested the parties to submit declarations of persons who could assist the court in understanding how far in advance of release the record companies generally knew that a particular recording would be released on a specific date.²²⁷⁵ Finally, the parties disagreed as to the present and future capabilities of the Napster system to screen the plaintiffs' copyrighted works. The court appointed a neutral expert, Dr. A. J. Nichols, to serve as a technology advisor in the matter, and requested that he work with the parties' technology experts and prepare a report to the court on the present and future capabilities of the Napster system to screen the plaintiffs' copyrighted works.²²⁷⁶

15. The July 11, 2001 Oral Modification of the Preliminary Injunction. Even after the Apr. 26 clarification, the parties continued to dispute bitterly the scope of the obligation on the part of the plaintiffs to supply filenames to Napster, as well as Napster's compliance with the modified preliminary injunction. The plaintiffs alleged that infringing files were still rampant on the Napster system, while Napster insisted that it was adequately blocking all filenames of which it had been made aware by the plaintiffs, as well as many variants of those filenames, including all files containing the names of many particular artists that had been noticed as illegally appearing on the system, and all files having titles or variants of those titles alleged to be infringing, regardless of the artist performing a work by that title – thereby resulting in substantial "overblocking" of files on the system.

During the months ensuing after the Apr. 26 clarification, Dr. Nichols issued a series of reports to the district court concerning Napster's ability to remove infringing files from its system. Also during this time, Napster voluntarily developed and switched to a new technology known as "fileID" for blocking allegedly infringing files from the Napster system. The new technology, unlike the old, was not based primarily on filenames, but rather on a technical analysis of the digital musical content contained in a file, including acoustic waveform recognition, to generate a "fingerprint." The parties disputed the effectiveness of the new technology and whether Napster's use of this technology was sufficient to comply with the

²²⁷³ Memorandum at 2.

²²⁷⁴ Id.

²²⁷⁵ Id.

²²⁷⁶ Id.

modified preliminary injunction. The plaintiffs insisted that the preliminary injunction required Napster's system to be 100% free of infringing files, and that there was still infringing material being shared through the system. Napster insisted, however, that no technology could ever be 100% accurate in screening out allegedly infringing materials from its system, and that neither the preliminary injunction, nor the Ninth Circuit's decision in Napster I, required its system to be 100% infringement free. Instead, Napster insisted that it was required to exert only reasonable efforts to block infringing material from its system, and only within the limits of the architecture of its system.

On July 1, 2001, Napster voluntarily shut down the file sharing operation of its system, after discovering flaws in its fileID fingerprinting technology, and conducted testing on its technology between July 2 and 9. The parties' disputes over Napster's compliance with the Mar. 5 modified injunction came to a head at a status conference before the district court on July 11, 2001. At that hearing, Napster told the court that, based on its testing, its newly implemented fileID technology was more than 99% effective and that it was prepared to resume allowing file sharing through its system.²²⁷⁷

The district court rejected Napster's proposal to resume file sharing, stating from the bench, "I think we're at a point where it has to stay that way [i.e., file sharing shut down] until you satisfy Dr. Nichols and me that when the system goes back up it will be able to block out or screen out copyrighted works that have been noticed."²²⁷⁸ Napster pressed the district court to clarify whether the Mar. 5 modified injunction was meant to require its system to be 100% accurate in screening of allegedly infringing materials. The court ruled orally as follows: "It's not good enough until every effort has been made to, in fact, get zero tolerance. Now that has to be the objective. If there's a little – it gets a little messy around edges, if there are some glitches and so forth, I can understand that. But this system is not going to go back up in such a manner as to permit copying and downloading other than to test that for the purposes of determining the error rate until you've satisfied Dr. Nichols. And then, he can notify me."²²⁷⁹

The district court denied Napster's request to stay her oral modified order and Napster immediately requested the Ninth Circuit to issue a stay. On July 18, 2001, the Ninth Circuit ordered "that the order issued by the district court on July 11, 2001, in open court, modifying the Preliminary Injunction issued March 5, 2001, is hereby stayed pending a further order of this court."²²⁸⁰ Despite the stay of the district court's oral modified order, Napster chose not to resume file sharing through its system.

Both Napster and the plaintiffs pursued further appeals to the Ninth Circuit in view of the July 11 oral order. The Ninth Circuit consolidated those appeals with the earlier appeals of the

²²⁷⁷ "Napster Asks 9th Circuit to Modify 1 Order, Vacate Another," *Mealey's Cyber Tech & E-Commerce Litigation Reporter* (Aug. 2001) 4-5.

²²⁷⁸ *Id.* at 5.

²²⁷⁹ *Id.*

²²⁸⁰ Order, A&M Records, Inc. v. Napster, Inc., No. 01-16308 (9th Cir. July 18, 2001).

Mar. 5 modified injunction. Its opinion in the consolidated appeals is discussed in subsection 17 below.

16. Napster's Motions to Dismiss the Complaints of the Independent Artists and AMPAS. While the consolidated appeals were pending, Napster filed a motion to dismiss the complaints of various independent artists and labels and of AMPAS for failure to state a claim. Napster based its motion on the Ninth Circuit's opinion in Napster I, which Napster argued fundamentally altered copyright liability in the online context.²²⁸¹ Napster framed the basis for its motion as a pure question of law – whether notice is an element of contributory and vicarious copyright infringement – and rested the motion on the following two arguments:

First, Napster contends that [Napster I] held that the traditional formulation of constructive knowledge for contributory infringement does not apply in the digital realm. Instead, copyright liability may only be imposed when a computer service provider has actual knowledge of specific infringing files. Second, Napster believes that the Ninth Circuit held that notice is a required element for both contributory and vicarious infringement. This notice, Napster contends, must be provided (1) by plaintiffs (2) prior to suit and (3) must list specific infringing files. Additionally, Napster reads [Napster I] to limit liability for contributory and vicarious infringement to cases in which after receiving notice, Napster fails to disable the infringing material. Simply put, Napster believes that the Ninth Circuit carved out a special niche in copyright law for computer service providers.²²⁸²

In response, the district court ruled that “there is a simple answer to Napster’s ‘pure question of law.’ There is no requirement that plaintiffs allege that they provided notice of specific infringing works prior to filing suit. The court agrees that computer system operators cannot be held liable for secondary copyright liability based *solely* on the transmission of unidentified (and unidentifiable) material through a computer system. To do otherwise would violate the basic tenet of Sony. However, according to plaintiffs’ complaints, Napster has gone far beyond simply providing a peer-to-peer file sharing system; it has engaged in music piracy of magnificent proportions.”²²⁸³ Accordingly, the court concluded that the plaintiffs had sufficiently pleaded the elements of contributory and vicarious infringement, and denied Napster’s motion.²²⁸⁴

The court based its conclusions on various significant interpretations of the Napster I opinion with respect to contributory and vicarious liability. With respect to contributory liability, the court noted that under Napster I, the secondary infringer must “know or have reason to know” of the direct infringement; “[a]ctual knowledge is not required; a defendant may possess

²²⁸¹ Fonovisa v. Napster, Inc., 2002 U.S. Dist. LEXIS 4270 at *11 (N.D. Cal. Jan. 28, 2002).

²²⁸² Id. at *11-12.

²²⁸³ Id. at *38-39 (emphasis in original).

²²⁸⁴ Id. at *39.

constructive knowledge if he has reason to know a third party's direct infringement."²²⁸⁵ The district court rejected Napster's argument that Napster I created a stricter standard of knowledge for service providers in an online context – namely, actual knowledge in the form of notice of specific copyrighted works from the plaintiffs prior to suit. Napster argued that it could not be held liable until such notice was given because its duty under Napster I to disable the offending material arose only after the plaintiffs provided notice.²²⁸⁶ The court ruled that "[c]ontrary to Napster's contention, Napster I did not create a new knowledge standard for contributory infringement. Instead, the court relied on the traditional formulation that either constructive or actual knowledge is sufficient to impose liability on Napster for contributory infringement."²²⁸⁷

The district court acknowledged some lack of clarity in the Ninth Circuit's Napster I opinion on the issue of knowledge, as discussed earlier in this paper: "The court is aware that the Ninth Circuit's reference to actual knowledge and failure to remove access might lead to some confusion. Lacking a more definitive statement from the Court of Appeals, the court understands the Ninth Circuit to hold that a range of conduct, when linked to Napster's system, may give rise to constructive or actual knowledge. Conduct sufficient for liability may take forms other than as a combination of actual knowledge and failure to block access. ... Plaintiffs allege that Napster knew of music piracy on its system, that it had the ability to patrol its database, that Napster had knowledge of some specific infringing files, and did nothing to prevent continued infringement. If these allegations are true, plaintiffs are entitled to at least preliminary injunctive relief under the reasoning of [Napster I]."²²⁸⁸

With respect to vicarious liability, the court noted that Napster had not challenged the plaintiffs' allegations of control and financial interest, but instead had argued that notice is an additional required element for both vicarious and contributory copyright infringement on the part of online service providers.²²⁸⁹ The court therefore turned to the issue of notice as a separate element of secondary infringement. Napster based its notice argument on the Ninth Circuit's modification in Napster I of the district court's original July 2000 preliminary injunction as being overbroad and its statement that "the burden [is] on plaintiffs to provide notice to Napster of copyrighted works and files containing such works available on the Napster system before Napster has the duty to disable access to the offending content."²²⁹⁰ Napster argued that this statement mandated notice as a necessary element of secondary infringement, and that any

²²⁸⁵ Id. at *14-15.

²²⁸⁶ Id. at *15-16.

²²⁸⁷ Id. at *16.

²²⁸⁸ Id. at *23-24.

²²⁸⁹ Id. at *26.

²²⁹⁰ Id. at *28-29 (quoting Napster I, 239 F.3d at 1027).

complaint failing to allege both notice prior to suit and Napster's subsequent failure to disable infringing material was deficient.²²⁹¹

The district court found Napster's interpretation of the Ninth Circuit's opinion to be problematic:

First, Napster reads the statement out of context. The burden-shifting statement upon which Napster relies addressed only the scope of injunctive relief. The Ninth Circuit was clearly concerned with the overbreadth of the injunction and believed that any liability based solely on the architecture of Napster's system implicated Sony. In tailoring injunctive relief to avoid violating Sony, the Ninth Circuit shifted the burden to plaintiffs to provide notice of specific infringing works and files. This burden-shifting alleviated concerns that Napster was being penalized simply because of its peer-to-peer file sharing system. More fundamentally, the Ninth Circuit's modification balanced the broad equitable discretion of this court with the doctrine that injunctive relief should avoid prohibiting legitimate conduct. ... Simply put, the Ninth Circuit's burden-shifting is case-specific, designed to alleviate Sony concerns.²²⁹²

Moreover, the district court was troubled that Napster's argument might imply that even if it had actual knowledge of specific infringement, Napster could simply wait until the plaintiffs discovered the infringement and then remove the offending files. The court believed such an argument would turn copyright law on its head and encourage willful blindness.²²⁹³ Finally, the court expressed the belief that, had the Ninth Circuit intended to overhaul copyright liability and carve out special protections for computer service providers, "it would have explicitly stated such a change."²²⁹⁴ Accordingly, the court concluded that the plaintiffs had adequately pleaded claims for contributory and vicarious liability.²²⁹⁵

17. The Second, Consolidated Appeal to the Ninth Circuit. In the second appeal to the Ninth Circuit, Napster argued that the notification requirements imposed on the plaintiffs by the Mar. 5 modified injunction were mandated by the Ninth Circuit's opinion in Napster I, and that even if they were not, their imposition was not an abuse of discretion by the district court.

²²⁹¹ Fonovisa v. Napster, 2002 U.S. Dist. LEXIS 4270, at *29.

²²⁹² Id. at *30.

²²⁹³ Id. at *31.

²²⁹⁴ Id. at *33. The court also rejected Napster's interpretation of the Netcom decision, discussed in Section II.A.4(a) above, as requiring notice of specific infringing files prior to filing suit. "Notice was an issue in Netcom only because notice was the means by which Netcom acquired knowledge of infringement. It was undisputed that prior to notice Netcom did not have the requisite knowledge for contributory infringement. ... [T]he issue in the present actions is not how Napster came by knowledge of infringement, but whether such knowledge exists." Id. at *35-36. The district court found the Ninth Circuit's reading of Netcom in Napster I to be in accord. "The Ninth Circuit noted that the situation in Netcom, where a computer service provider has actual knowledge of specific infringing files, is *sufficient* to give rise to liability. The court never stated that actual knowledge (or notice for that matter) was *necessary* for liability." Id. at *36-37 (emphasis in original).

²²⁹⁵ Id. at *39.

However, Napster argued that the policing obligations of the Mar. 5 modified injunction were too indeterminate to meet the requirements of Rule 65 of the Federal Rules of Civil Procedure, because the Mar. 5 order did not specify the extent, and at what cost, Napster was required to discharge its policing obligations. Unless clarified, Napster argued that the policing obligations would potentially authorize massive blocking of noninfringing works. Napster also argued that the Mar. 5 order impermissibly delegated judicial functions to Dr. Nichols.²²⁹⁶

With respect to the July 11 oral order, Napster argued that the district court lacked jurisdiction to issue the order because it constituted a modification of the Mar. 5 order, which was on appeal. Napster noted that the Ninth Circuit, in its stay order, had itself characterized the July 11 order as “modifying” the Mar. 5 order.²²⁹⁷ Napster also argued that, in any event, the July 11 order’s “zero tolerance” standard was fundamentally at odds with the Ninth Circuit ruling in Napster I.²²⁹⁸ The plaintiffs, in turn, challenged the requirements of the preliminary injunctions that they provide to Napster file names found on the Napster index that corresponded to their copyrighted works before Napster had a duty to act on those files.

On appeal, the Ninth Circuit rejected most of the arguments of both Napster and the plaintiffs in a very sparse opinion that will be referred to as “Napster II.”²²⁹⁹ With respect to the plaintiffs’ argument that it should not have to supply file names to Napster and that Napster should instead be required to search for and block all files containing any protected copyrighted works, not just works with which plaintiffs had been able to provide a corresponding file name, the Ninth Circuit ruled that the notice requirements of the preliminary injunctions complied with its holding in Napster I that the plaintiffs bore the burden to provide notice to Napster of copyrighted works and files containing such works before Napster had a duty to disable access to the offending content.²³⁰⁰ The court further held that “Napster’s duty to search under the modified preliminary injunction is consistent with our holding that Napster must ‘affirmatively use its ability to patrol its system and preclude access to potentially infringing files listed on its search index.’ The modified preliminary injunction correctly reflects the legal principles of contributory and vicarious copyright infringement that we previously articulated.”²³⁰¹ Thus, the Ninth Circuit’s Napster II opinion appears to establish a legal rule under which there is a notice requirement both for the imposition of common law contributory liability and vicarious liability

²²⁹⁶ “Napster Asks 9th Circuit to Modify 1 Order, Vacate Another,” *Mealey’s Cyber Tech & E-Commerce Litigation Reporter* (Aug. 2001) 5-6.

²²⁹⁷ Id. at 6.

²²⁹⁸ Id.

²²⁹⁹ A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002).

²³⁰⁰ Id. at 1096.

²³⁰¹ Id. at 1096-97 (quoting Napster I, 239 F.3d at 1027).

on an OSP, contrary to the district court's conclusion otherwise in its opinion on Napster's motion to dismiss, discussed in subsection 16 above.²³⁰²

The Ninth Circuit rejected Napster's challenge to the preliminary injunction as impermissibly vague. The court's very terse response was as follows: "Napster has a duty to police its system in order to avoid vicarious infringement. Napster can police the system by searching its index for files containing a noticed copyrighted work. The modified preliminary injunction directs Napster, in no vague terms, to do exactly that."²³⁰³ The court also rejected Napster's argument that the district court had improperly delegated its judicial authority to Dr. Nichols: "At no time did the technical advisor displace the district court's judicial role. The technical advisor never unilaterally issued findings of fact or conclusions of law regarding Napster's compliance."²³⁰⁴

Next, the court turned to Napster's challenge that the shutdown order improperly amended the modified preliminary injunction by requiring a non-text-based filtering mechanism and a "zero tolerance" standard for compliance. The Ninth Circuit rejected each of these challenges. The court apparently found that the requirement of a non-text-based filtering mechanism did not violate the court's ruling in Napster I that Napster's duty to policy was "cabined by the system's current architecture,"²³⁰⁵ because the new filtering mechanism "still requires Napster to search files located on the index to locate infringing material."²³⁰⁶ Thus, the court appears to have viewed the "architecture" of the Napster system as *index* based, rather than *text* based.²³⁰⁷ Moreover, the Ninth Circuit noted that a district court has inherent authority to modify a preliminary injunction in consideration of new facts. "The text-based filter proved to be vulnerable to user-defined variations in file names. The new filtering mechanism, on the other hand, does not depend on file names and thus is not similarly susceptible to bypass. It was a proper exercise of the district court's supervisory authority to require use of the new filtering mechanism, which may counter Napster's inability to fully comply with the modified

²³⁰² This rule would not, however, appear to survive the Supreme Court's decision in Metro-Goldwyn-Mayer Studios Inc. v. Gorkster, Ltd., 545 U.S. 913, 919 (2005), discussed in Section III.C.4(a) below.

²³⁰³ Napster II, 284 F.3d at 1097.

²³⁰⁴ Id.

²³⁰⁵ Napster I, 239 F.3d at 1024.

²³⁰⁶ Napster II, 284 F.3d at 1098.

²³⁰⁷ It appears that the Ninth Circuit did not fully understand the non-text-based filtering mechanism that the district court required Napster to use. As discussed in subsection 15, that alternative filtering technology known as "fileID," unlike the old technology, was not based primarily on textual filenames, but rather on a technical analysis of the digital musical content contained in a file, including acoustic waveform recognition, to generate a "fingerprint." Napster *combined* the fileID technology with its textual filename search technology using the index, but the fileID technology required a fundamentally different approach to identifying potentially infringing works. However, the fact that Napster continued to maintain an index appears to have led the Ninth Circuit to conclude rather facily that requiring the use of fileID technology did not constitute a departure from the original Napster system "architecture," when in fact it required a radically different approach.

preliminary injunction.”²³⁰⁸ This is a substantial ruling, as it appears to allow a district court to require an OSP to adopt new technologies that may become available in order to keep infringing materials off its system.

With respect to the “zero tolerance” challenge, the Ninth Circuit ruled that the district court’s imposition of a “zero tolerance” standard was permissible because that standard did not apply to all potentially infringing works on Napster’s system, but only to those works that had been noticed by the plaintiff:

The district court did not, as Napster argues, premise the shut down order on a requirement that Napster must prevent infringement of all of plaintiffs’ copyrighted works, without regard to plaintiffs’ duty to provide notice. The tolerance standard announced applies only to copyrighted works which plaintiffs have properly noticed as required by the modified preliminary injunction. That is, Napster must do everything feasible to block files from its system which contain noticed copyrighted works. ... The district court determined that more could be done to maximize the effectiveness of the new filtering mechanism. Ordering Napster to keep its file transferring service disabled in these circumstances was not an abuse of discretion.²³⁰⁹

Even with this clarification of the “zero tolerance” standard, the Ninth Circuit’s allowance of that standard may pose a formidable challenge for many OSPs seeking to avoid liability for copyright infringement. It seems unlikely that any technology for identifying and blocking infringing works on a system will be completely foolproof. And how far must an OSP go to do “everything feasible” to block noticed copyrighted works – must it constantly upgrade its technology to the most leading, perhaps unproven, technology? Where is the line on what is “feasible”?

Finally, the Ninth Circuit rejected Napster’s challenge that the district court lacked authority to modify the preliminary injunction pending appeal. The court noted that, although a district court cannot, while a preliminary injunction is on appeal, modify the injunction in such manner as to finally adjudicate substantial rights directly involved in the appeal, it can, under Federal Rule of Civil Procedure 62(c), continue supervision of compliance with the injunction. The Ninth Circuit ruled that the district court had properly exercised its power under this Rule.²³¹⁰ Accordingly, the court affirmed both the modified preliminary injunction and the shut down order, noting that the “shut down order was a proper exercise of the district court’s power to enforce compliance with the modified preliminary injunction.”²³¹¹

18. Motions for Summary Judgment and for Discovery on Misuse Theory and Ownership Questions. While the second consolidated appeal was pending, the plaintiffs filed motions in the

²³⁰⁸ Id. at 1098.

²³⁰⁹ Id.

²³¹⁰ Id. at 1099.

²³¹¹ Id.

district court for summary judgment of willful contributory and vicarious copyright infringement. Napster requested, pursuant to Rule 56(f) of the Federal Rules of Civil Procedure, that the court stay any decision on the merits to allow for additional discovery on the questions of (i) whether the plaintiffs actually owned the rights to the musical works for which they alleged infringement and (ii) whether the plaintiffs had misused their copyrights by attempting to control the market for the digital distribution of music.²³¹²

With respect to the ownership issues, the plaintiffs rested on the legal rule that a copyright certificate establishes prima facie evidence of the validity of a copyright and the facts in the certificate.²³¹³ Napster challenged the presumption of ownership set up by the certificates, arguing that in 133 of the 144 copyright certificates submitted with the complaint, the registered works were incorrectly designated as “works for hire.” The plaintiffs, in turn, challenged Napster’s standing to challenge the presumption of ownership. The court noted a line of cases holding that a third party does not have standing to challenge the presumption of ownership when a plaintiff claims ownership by assignment, but ruled that the third-party standing doctrine does not apply in instances of ownership by authorship. Accordingly, Napster had standing to challenge whether the works in suit were works for hire.²³¹⁴

The court held that there were substantial questions raised by Napster on which it was entitled to take discovery with respect to whether the plaintiffs could satisfy either of the two prongs of the definition of “work made for hire.”²³¹⁵ With respect to the “specially commissioned” prong of the definition, the court noted that sound recordings are not one of the nine types of specially commissioned works listed in the definition that can qualify as works made for hire. With respect to the “employment” prong of the definition, the court noted that the plaintiffs had produced no contracts with artists to demonstrate an employment

²³¹² *In re Napster Inc. Copyright Litigation*, 191 F. Supp. 2d 1087, 1093 (N.D. Cal. 2002). Napster also alleged that there were disputed issues of fact with respect to “plaintiffs’ ownership of the copyrighted works at issue, copying of the works, fair use, the application of *Sony*, the extent of Napster’s control over its system and its policing obligation, the extent of the Napster system’s architecture, the sufficiency of plaintiffs’ notices and Napster’s removal of those works, application of the Digital Millennium Copyright Act, copyright misuse, and willfulness.” *Id.* at 1095 n.1.

²³¹³ 17 U.S.C. § 410(c).

²³¹⁴ *In re Napster Copyright Litigation*, 191 F. Supp. 2d at 1097-98.

²³¹⁵ 17 U.S.C. § 101 defines a “work made for hire” as “(1) a work prepared by an employee within the scope of his or her employment; or (2) a work specially ordered or commissioned for use as a contribution to a collective work, as a part of a motion picture or other audiovisual work, as a translation, as a supplementary work, as a compilation, as an instructional text, as a test, as answer material for a test, or as an atlas, if the parties expressly agree in a written instrument signed by them that the work shall be considered a work made for hire. For the purpose of the foregoing sentence, a ‘supplementary work’ is a work prepared for publication as a secondary adjunct to a work by another author for the purpose of introducing, concluding, illustrating, explaining, revising, commenting upon, or assisting in the use of the other work, such as forewords, afterwords, pictorial illustrations, maps, charts, tables, editorial notes, musical arrangements, answer material for tests, bibliographies, appendixes, and indexes, and an ‘instructional text’ is a literary, pictorial, or graphic work prepared for publication and with the purpose of use in systematic instructional activities.”

relationship.²³¹⁶ The court ordered the plaintiffs to produce all documentation relevant to their ownership of the works listed as works for hire to a Special Master appointed by the court to review them. The court specifically withheld any rulings on the work for hire issue, the scope of the plaintiffs' rights, and the extent to which the plaintiffs were protected by the presumption of ownership until further discovery was completed.²³¹⁷

The court then turned to Napster's need for discovery on its allegations of copyright misuse by the plaintiffs. The court first noted that, although both itself and the Ninth Circuit had dismissed Napster's misuse defense at the preliminary injunction stage, "[s]ince those rulings, the factual and procedural landscape has changed significantly. ... The evidence now shows that plaintiffs have licensed their catalogs of works for digital distribution in what could be an overreaching manner. The evidence also suggests that plaintiffs' entry into the digital distribution market may run afoul of the antitrust laws."²³¹⁸

Napster based its allegations of misuse on unduly restrictive licensing requirements of the plaintiffs' online music venture, MusicNet, with which Napster had entered into a license agreement. That agreement prevented Napster from entering into any licensing agreement with any individual plaintiffs until March 1, 2002 and provided that even after March 2002, if Napster entered into any individual license with any of the plaintiffs, MusicNet could terminate the agreement upon 90 days' notice. Additionally, the license set up a pricing structure under which Napster would be charged higher fees if it failed to use MusicNet as its exclusive licensor for content.²³¹⁹ The court held that these provisions effectively granted MusicNet control over which content Napster licensed. "The result is an expansion of the powers of the three MusicNet plaintiffs' copyrights to cover the catalogs of the two non-MusicNet plaintiffs."²³²⁰ The court noted that further inquiry into the actions of MusicNet, and whether those actions should be imputed to the plaintiffs, was warranted.²³²¹

²³¹⁶ In re Napster Copyright Litigation, 191 F. Supp. 2d. at 1098.

²³¹⁷ Id. at 1100. The court further ruled that, with respect to works listing an author other than the plaintiffs on the registration certificate and works protected under state law, the plaintiffs would be obliged to produce a chain of title from the listed author to themselves. Id. at 1101. Works with pending registrations would be given the benefit of the presumption of ownership. Id. Finally, for those works for which the plaintiffs had not yet filed an application for registration, the court ruled that it lacked subject matter jurisdiction. Id.

²³¹⁸ Id. at 1102 (citations omitted).

²³¹⁹ Id. at 1105-06.

²³²⁰ Id. at 1106.

²³²¹ Id. at 1107. The court further noted that, if the plaintiffs were engaged in misuse, they could not bring suit based on their rights until the misuse ended, although the misuse would not ultimately preclude recovery for infringement: "The doctrine [of misuse] does not prevent plaintiffs from ultimately recovering for acts of infringement that occur during the period of misuse. The issue focuses on when plaintiffs can bring or pursue an action for infringement, not for which acts of infringement they can recover." Id. at 1108.

The court also found that Napster had raised substantial issues of whether the plaintiffs' entry into the digital distribution market constituted antitrust violations. "[E]ven a naïf must realize that in forming and operating a joint venture, plaintiffs' representatives must necessarily meet and discuss pricing and licensing, raising the specter of possible antitrust violations. These joint ventures bear the indicia of entities designed to allow plaintiffs to use their copyrights and extensive market power to dominate the market for digital music distribution. Even on the undeveloped record before the court, these joint ventures look bad, sound bad and smell bad."²³²² Accordingly, the court granted Napster's Rule 56(f) motion for further discovery into the antitrust and misuse issues raised by Napster.²³²³ Such discovery was subsequently stayed as the result of filing of bankruptcy by Napster in June of 2002. On August 9, 2002, Napster's assets were placed up for auction in the bankruptcy proceeding.²³²⁴

(2) The Scour.com Lawsuit

Another case challenged the legality of peer-to-peer file sharing through a service similar to the Napster service. On July 20, 2000, several leading motion picture studios, record companies, and music publishers filed a copyright infringement action in federal district court in New York against Scour, Inc., operator of an online file sharing service known as the Scour Exchange. Unlike the Napster service, which was limited to the exchange of music files in MP3 format, the Scour Exchange enabled the peer-to-peer exchange of both music and motion picture files among the hard drives of Scour users. The Scour website featured a banner containing a "Top Five" search list, identifying current hit motion picture titles and music recordings that had been requested most frequently by Scour users.²³²⁵

Like the Napster service, Scour's website provided users with free copies of its proprietary file sharing software, which users could use to connect to Scour's servers and choose which content files stored on their computer hard drives they wished to make available for other Scour users to download. Scour then inventoried the files each user had so designated and combined them in a database and directory that was made available on Scour's servers to all Scour users currently logged on. Users could search the directory and initiate downloads of

The court also rejected the plaintiffs' argument that Napster should not be allowed to assert a misuse defense because of its own unclean hands. Because the plaintiffs had themselves sought equitable relief from the court, Napster should not be barred from bringing an equitable defense. *Id.* at 1110-11. In any event, upon a balancing of equities, the court concluded that "the potential for public injury and the fact that Napster has shut its doors to infringement justifies allowing Napster to assert a misuse defense to obtain additional discovery." *Id.* at 1113.

²³²² *Id.* at 1109 (citations omitted).

²³²³ *Id.* at 1113.

²³²⁴ Scarlett Pruitt, "Napster Assets Go Up for Auction" (Aug. 12, 2002), available as of Aug. 12, 2002 at www.infoworld.com/articles/hn/xml/02/08/12/020812hnapster.xml.

²³²⁵ Complaint, *Twentieth Century Fox Film Corp. v. Scour, Inc.*, No. 00 Civ. 5385 (GBD) (S.D.N.Y., filed July 20, 2000) ¶¶ 1-2, available as of Dec. 16, 2000 at www.mpa.org/press/scourcomplaint.htm.

desired material from other users' computers.²³²⁶ Unlike Napster, however, Scour also made available through a partnership with a third party a service that provided secure storage space for files on a remote server. The service provided what Scour promoted as "free, secure, online storage space for all the multimedia files that you find on Scour." Through this service, Scour users were able to upload their files onto this remote server for other Scour users to download, regardless of whether the originating user was logged on to Scour's servers.²³²⁷ The plaintiffs alleged that Scour was contributorily and vicariously liable for the infringing downloads of copyrighted material by Scour's users.²³²⁸

The defense of the lawsuit proved too costly for Scour, and on October 13, 2000, Scour filed for Chapter 11 bankruptcy protection.²³²⁹ On Nov. 14, 2000, Scour announced that it would shut down its exchange service in order facilitate a resolution of the copyright infringement litigation and the sale of its assets, which Listen.com had offered to purchase for \$5 million in cash and more than 500,000 shares of stock.²³³⁰

(3) The Aimster/Madster Lawsuits

On April 30, 2001 a company called Aimster, which was operating a file swapping service very similar to the Scour service, filed suit in federal court in Albany, New York against various members of the RIAA for a declaratory judgment that it was not secondarily liable for copyright infringement by users of its service to swap allegedly infringing material. The Aimster service was based on a peer-to-peer technology, but was different from Napster and Scour in that files were traded in an encrypted format which Aimster claimed prevented it from having knowledge of when its users were exchanging files, the identity of persons exchanging files, or what files were being exchanged through its service.²³³¹

The Aimster service was based on instant messaging (IM) technology from AOL. Specifically, Aimster made use of AOL IM's "get file" functionality, which gave AOL IM users the ability to designate certain files or directories on the user's hard drive that would be made available for other IM users to copy. The native "get file" functionality in AOL was limited in two ways. First, a user could retrieve files only from a list of his or her known "buddies" who were logged on at the same time. Second, there was no capability to search the files that were

²³²⁶ *Id.* ¶ 58.

²³²⁷ *Id.* ¶ 60.

²³²⁸ *Id.* ¶ 71.

²³²⁹ Jim Hu, "Scour Files for Bankruptcy Protection" (Oct. 13, 2000), available as of Dec. 16, 2000 at <http://news.cnet.com/news/0-1005-200-3178822.html>.

²³³⁰ Steven Musil, "Scour to End File-Swapping Service" (Nov. 14, 2000), available as of Dec. 16, 2000 at <http://news.cnet.com/news/0-1005-200-3689821.html>.

²³³¹ *In re Aimster Copyright Litigation*, 252 F. Supp. 2d 634, 641 (N.D. Ill. 2002).

available from a buddy; the user was required to know the particular file that was being sought on the buddy's hard drive before that file could be fetched.²³³²

The Aimster service considerably expanded upon the basic file transferring capability of the AOL IM system by designating every Aimster user as the buddy of every other Aimster user, thereby allowing all Aimster users to communicate and share files with any other Aimster user currently online. The Aimster service also afforded its users the capability to search all the files contained on the hard drives of other users that had been designated for sharing.²³³³ Once the search for a suitable file was complete, an Aimster user needed only to click on the file name title and then click on a "Download" button to obtain a copy of the song. The Aimster system then facilitated the connection of its two users through a private, encrypted network so the file could be transferred. During the copying of a file, the Aimster system provided a constant update about the status of each download or upload.²³³⁴

The Aimster service contained several additional features that ultimately proved relevant to the analysis of copyright infringement. First, located for a time on Aimster's web site was a utility called "Aimster's Guardian Tutorial," which demonstrated how to transfer and copy copyrighted works over the Aimster system using as illustrative on-screen examples some of the copyrighted works of RIAA members. Second, Aimster's service offered message boards on which Aimster users wishing to download particular copyrighted recordings could seek the assistance of others. In addition, users often posted messages on these boards openly discussing trafficking in copyrighted material and "screwing" the RIAA.²³³⁵ Finally, in November 2001, Aimster launched a service called "Club Aimster," which required a \$4.95 monthly service fee, for which users were given access to a list of "The Aimster Top-40," a list of the 40 "hot new releases" most frequently downloaded by Aimster users, virtually all of which were owned by RIAA members. Each Aimster Top 40 selection included a Play button that a user could click to automatically begin the copying and transfer of that particular song to the user's computer without the inconvenience of having to type in an Aimster search request. At one point, Aimster changed its procedures to require all prospective users to join Club Aimster in order to be able to download the Aimster client software.²³³⁶

On May 24, 2001, various members of the RIAA responded to Aimster's declaratory judgment lawsuit by filing copyright infringement lawsuits against BuddyUSA and AbovePeer, corporate entities that owned the Aimster software and file swapping service, and Johnny Deep,

²³³² Id. at 640.

²³³³ Id. at 642. The parties hotly disputed whether Aimster catalogued all available files for download in a single, centralized database, akin to the Napster system. In issuing its preliminary injunction, the court noted that its legal analysis of the copyright issues would hold regardless of whether or not Aimster maintained a central database of files available for transfer. Id. at 641 n.6.

²³³⁴ Id. at 642-43

²³³⁵ Id. at 643-44, 650.

²³³⁶ Id. at 644-45.

CEO of Aimster, in federal court in Manhattan.²³³⁷ On May 29, 2001, these lawsuits were stayed by the court in Albany,²³³⁸ although the stay was lifted on June 22.²³³⁹ On June 27, seven major motion picture studios also filed suit against Deep, BuddyUSA and AbovePeer alleging copyright infringement based on the ability of the Aimster service to share copyrighted motion pictures.²³⁴⁰ In July 2001 various music publishers and songwriters joined the fray with their own copyright infringement lawsuit filed in Manhattan.²³⁴¹ On Nov. 19, 2001, a multi-jurisdictional panel of judges in San Diego ruled that the bevy of lawsuits against Aimster should be tried in federal district court in Chicago as a convenient, central forum among all the various parties.²³⁴²

On Mar. 19, 2002, the lawsuits against the Aimster service, which was subsequently renamed “Madster” after a trademark dispute with AOL, were placed on hold after BuddyUSA and AbovePeer filed for bankruptcy. On June 20, 2002, the bankruptcy judge lifted the automatic stay of the lawsuits to the extent necessary to allow the record companies to pursue a preliminary injunction against the service in the federal district court in Chicago.²³⁴³ About three months later, the district court ruled that the plaintiffs were entitled to a preliminary injunction on grounds of contributory and vicarious liability.²³⁴⁴ Aimster appealed.

The Seventh Circuit, per Judge Posner, affirmed the issuance of the preliminary injunction, finding that Aimster was likely liable as a contributory infringer.²³⁴⁵ The bulk of the

²³³⁷ *Id.* at 646.

²³³⁸ Steven Bonisteel, “Aimster in Court Today to Fend Off Music-Industry Suits” (May 30, 2001), available as of Jan. 6, 2002 at www.newsbytes.com/news/01/166250.html.

²³³⁹ Michael Bartlett, “Movie Studios Attack File-Swapping Service Aimster” (July 3, 2001), available as of Jan. 6, 2002 at www.newsbytes.com/news/01/167549.html.

²³⁴⁰ *Id.*

²³⁴¹ “Aimster: Another Day, Another Lawsuit” (July 5, 2001), available as of Jan. 6, 2002 at www.usatoday.com/life/cyber/tech/2001-07-05-aimster.htm.

²³⁴² Kevin Featherly, “Judges Consolidate Aimster Suits – Correction” (Nov. 19, 2001), available as of Jan. 6, 2002 at www.newsbytes.com/news/01/172294.html.

²³⁴³ “Judge: Record Companies Can Pursue Injunction Against Madster” (June 21, 2002), available as of June 21, 2002 at www.siliconvalley.com/mld/siliconvalley/news/editorial/3511564.htm.

²³⁴⁴ *In re Aimster Copyright Litigation*, 252 F. Supp. 2d 634, 665 (N.D. Ill. 2002). The district court also rejected Aimster’s argument of a defense under the AHRA. The court first ruled that Aimster’s users were plainly engaged in direct copyright infringement and that the AHRA did not provide an affirmative defense to the users’ acts of direct copying. Invoking the Ninth Circuit’s *Diamond Multimedia* decision, discussed extensively in Section III.C.2(c)(1).2 above, Aimster argued that the AHRA immunized all noncommercial copying by consumers of digital and analog musical recordings. The district court rejected this argument, distinguishing *Diamond Multimedia* on the grounds that in that case users were merely space shifting files from their hard drives to a portable digital device for their own personal use. By contrast, the Aimster service involved the copying of MP3 files from one user’s hard drive onto the hard drive of another user, and such massive, unauthorized distribution and copying of the plaintiffs’ works was not within the scope of the AHRA. *Id.* at 648-49.

²³⁴⁵ *In re Aimster Copyright Litigation*, 334 F.3d 643 (7th Cir. 2003), *cert. denied*, 124 S. Ct. 1069 (2004).

court's opinion was devoted to an analysis of the scope of the Supreme Court's "substantial noninfringing use" doctrine in the Sony case, on which Aimster relied heavily for its defense. Judge Posner seems to have significantly reinterpreted that doctrine using a classic "Chicago school" law and economics analysis. (The viability of Judge Posner's interpretive approach to Sony's "substantial noninfringing use" doctrine, whether or not it led to the correct substantive outcome, is at best dubious after the Supreme Court's Grokster decision discussed in Section III.C.2(c)(5) below.²³⁴⁶)

He began the analysis by noting that Sony's Betamax video recorder was used for three principal purposes – time shifting (recording a television program for later viewing), library building (making copies of programs to retain permanently), and commercial skipping (taping a program before watching it and then, while watching the tape, using the fast-forward button on the recorder to skip over the commercials).²³⁴⁷ He noted that the Supreme Court held the first use to be a fair use because it enlarged the audience for the program, but went on to note, in dicta, that the second and third uses were "unquestionably infringing" – the second because "it was the equivalent of borrowing a copyrighted book from a public library, making a copy of it for one's personal library, then returning the original to the public library," and the third because it "amounted to creating an unauthorized derivative work ... namely a commercial-free copy that would reduce the copyright owner's income from his original program, since 'free' television programs are financed by the purchase of commercials by advertisers."²³⁴⁸ Thus, according to Judge Posner, the Supreme Court in Sony was confronted with a situation in which the video recorder "was being used for a mixture of infringing and noninfringing uses and the Court thought that Sony could not demix them because once Sony sold the recorder it lost all control over its use."²³⁴⁹

Having characterized the Sony case thusly, Judge Posner turned to an application of its principles to the Aimster service. He first rejected some extreme interpretations of those principles put forward by the parties. Specifically, he rejected the RIAA's argument that Sony is inapplicable to services and that, where services are concerned, "the test is merely whether the provider knows it's being used to infringe copyright."²³⁵⁰ He noted that although knowledge that

²³⁴⁶ See Mitchell Zimmerman, "Grokster Seems Unlikely to Prevent File Sharing by Itself," *The Daily Journal* (Aug 15, 2005).

²³⁴⁷ Id. at 647.

²³⁴⁸ Id. at 647-48. The ruling that recording for commercial skipping constitutes the making of an unauthorized derivative work is curious. First, it seems novel to judge the legality of a reproduced work on the *subsequent potential use* that a user may put the work to. Second, the work that was actually fixed in the tangible medium by the video recorder was the entire television program, including the commercials without modification. It is only upon playback that the commercials were skipped by fast forwarding through them, and one would have to argue that the transient display produced on the television screen as the commercials run by at faster speed is itself a derivative work. And even if a derivative work, it is unclear why such work might not be a fair use, at least when done by a private viewer to enhance enjoyment of the program.

²³⁴⁹ Id. at 648.

²³⁵⁰ Id.

a service is being used for infringing purposes is a factor to be considered in contributory infringement, it cannot be dispositive, else services like AOL's instant messaging service would be illegal just because some use it for infringing purposes.²³⁵¹ Moreover, he noted that in the Sony case, the Supreme Court acknowledged that 25% of Betamax users were fast forwarding through commercials, which, as noted, Judge Posner believed to constitute an infringing use, yet nevertheless there was no contributory infringement.²³⁵² Judge Posner thus concluded, "We therefore agree with Professor Goldstein that the Ninth Circuit erred in *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1020 (9th Cir. 2001), in suggesting that actual knowledge of specific infringing uses is a sufficient condition for deeming a facilitator a contributor infringer."²³⁵³

Conversely, Judge Posner rejected Aimster's argument that any showing that its service *could* be used in noninfringing ways is sufficient to avoid contributory liability. "Were that the law, the seller of a product or service used *solely* to facilitate copyright infringement, though it was capable in principle of noninfringing uses, would be immune from liability for contributory infringement."²³⁵⁴ In addition, the Supreme Court would not have thought it important to state that the Betamax was used "principally" for time shifting.²³⁵⁵

Judge Posner therefore interpreted the Sony doctrine ultimately to require an economic cost/benefit analysis of the infringing and noninfringing uses of a system in determining contributory liability. "What is true is that when a supplier is offering a product or service that has noninfringing as well as infringing uses, some estimate of the respective magnitudes of these uses is necessary for a finding of contributory infringement. ... But the balancing of costs and benefits is necessary only in a case in which substantial noninfringing uses, present or prospective, are demonstrated."²³⁵⁶

In the instant case, the court concluded the evidence showed that the Aimster system was principally for use for infringement. The court pointed to the fact that in explaining how to use the Aimster software, the tutorial gave as its only examples of file sharing the sharing of copyrighted music. In addition, membership in Club Aimster enabled the member for a fee of \$4.95 a month to download with a single click the 40 songs most often shared by Aimster users, and those were invariably copyrighted by the plaintiffs.²³⁵⁷ "The evidence that we have summarized does not exclude the *possibility* of substantial noninfringing uses of the Aimster system, but the evidence is sufficient, especially in a preliminary-injunction proceeding, which is

²³⁵¹ Id.

²³⁵² Id. at 649.

²³⁵³ Id. (citing 2 Paul Goldstein, *Copyright* § 6.1.2, p. 6:12-1 (2d ed. 2003)).

²³⁵⁴ 334 F.3d at 651.

²³⁵⁵ Id. (emphasis in original).

²³⁵⁶ Id. at 649-50.

²³⁵⁷ Id. at 651-52.

summary in character, to shift the burden of production to Aimster to demonstrate that its service has substantial noninfringing uses.”²³⁵⁸

The court held that Aimster had failed to show that its service had ever been used for a noninfringing use, let alone evidence concerning the frequency of such uses.²³⁵⁹ “Even when there are noninfringing uses of an Internet file-sharing service, moreover, if the infringing uses are substantial then to avoid liability as a contributory infringer the provider of the service must show that it would have been disproportionately costly for him to eliminate or at least reduce substantially the infringing uses.”²³⁶⁰ Not only had Aimster failed to engage in this calculation, the court ruled that it had willfully blinded itself from evidence of how its service was being used by providing encryption for all transactions on the service.²³⁶¹ “This is not to say that the provider of an encrypted instant-messaging service or encryption software is ipso facto[] a contributory infringer should his buyers use the service to infringe copyright Our point is only that a service provider that would otherwise be a contributory infringer does not obtain immunity by using encryption to shield itself from actual knowledge of the unlawful purposes for which the service is being used.”²³⁶²

The court therefore concluded that it was likely Aimster would be found a contributory infringer and affirmed the granting of the preliminary injunction.²³⁶³

The court also rejected a challenge to the injunction’s breadth. The preliminary injunction, which was very broad in sweep, required Aimster to “immediately disable and prevent any and all access” to the plaintiffs’ copyrighted works on or through any web site, server, or system owned or controlled by Aimster, “including, if necessary, preventing any and all access to the Aimster System and Service in its entirety, until such time that Aimster implements measures that prevent” unauthorized copying and downloading of the plaintiffs’ copyrighted works.²³⁶⁴ After implementing “measures to ensure that the Aimster System and Service prevents any and all copying, downloading, distributing, uploading, linking to, or transmitting” of the plaintiffs’ copyrighted works, Aimster was permitted to provide public access to its system,

²³⁵⁸ Id. at 652 (emphasis in original).

²³⁵⁹ Id. at 653.

²³⁶⁰ Id.

²³⁶¹ Id.

²³⁶² Id. at 650-51.

²³⁶³ Id. at 656. For a case post-dating the Supreme Court’s Grokster decision that interprets and applies Judge Posner’s tests for contributory infringement in a non-service provider context, see Monotype Imaging, Inc. v. Bitstream Inc., 2005 U.S. Dist. LEXIS 7410 (N.D. Ill. Apr. 21, 2005) (opinion on motion for summary judgment) and 2005 U.S. Dist. LEXIS 14278 (N.D. Ill. (July 12, 2005) (opinion after bench trial). The court in Monotype applied the Aimster approach to contributory liability without considering at all the issue of whether any of the rationale or holdings of the Aimster cases were called into question by the Supreme Court’s Grokster decision.

²³⁶⁴ Preliminary Injunction Order, In re Aimster Copyright Litigation, No. 01 c 8933 (N.D. Ill. Oct. 30, 2002) at ¶ 2.

except that it continued to be enjoined from copying, downloading or distributing the plaintiffs' copyrighted works or facilitating the same.²³⁶⁵

Aimster was also required to "affirmatively monitor and patrol for, and preclude access to" the plaintiffs' copyrighted works "by employing such technological tools and measures that are reasonably available to carry out such obligations" without specifying what those might be or what technical effectiveness criteria they would have to satisfy.²³⁶⁶ Finally, in one of the most onerous parts of the order, Aimster was required to "maintain a complete list of any and all sound recordings and musical compositions made available on, over, through, or via its system, and upon five (5) business days' notice [to] make such lists available to Plaintiffs for inspection and copying. Such lists shall include, without limitation, computer, website, and computer server logs delineating User search requests, download requests and upload attempts for any and all sound records and musical compositions."²³⁶⁷ The Seventh Circuit rejected Aimster's challenge to the breadth of the injunction on the ground that Aimster had failed to suggest alternative language either to the district court or to the Seventh Circuit, and had therefore waived the objection.²³⁶⁸

(4) The StreamCast/Kazaa/Grokster Lawsuits

One of the most significant peer-to-peer lawsuits to be filed after the Napster case involved the file sharing services originally known as Music City (later renamed to StreamCast), Kazaa, and Grokster. On Oct. 2, 2001, various recording companies and movie studios sued the operators of these services for copyright infringement in the Central District of California. Shortly thereafter, on Nov. 19, 2001, Jerry Leiber and Mike Stoller filed a class action for copyright infringement on behalf of themselves and all music publishers represented by The Harry Fox Agency against the same defendants, again in the Central District of California. The two lawsuits were eventually consolidated.

These suits presented a potential extension of the legal theories on which the Napster case relied in view of technical differences in the peer-to-peer architecture used by the StreamCast, Kazaa, and Grokster services, as opposed to the Napster service. As discussed in Section III.C.2(c)(1) above, the Napster service relied on a central index of files available for sharing stored on servers maintained and controlled by Napster. This index enabled Napster to block allegedly infringing files by searching the filenames available through the index. By contrast, the StreamCast, Kazaa, and Grokster services did not operate based on such a central index. Rather, the indexes of files available for sharing were distributed across users' computers.

Specifically, according to the complaint filed in the class action case, each of the StreamCast, Kazaa, and Grokster services initially relied on software called FastTrack, originally

²³⁶⁵ Id. ¶ 3.

²³⁶⁶ Id. ¶4.

²³⁶⁷ Id. ¶ 6.

²³⁶⁸ In re Aimster Copyright Litigation, 334 F.3d 643, 656 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004).

developed by a group of Scandinavian programmers known as Consumer Empowerment BV, later renamed Kazaa BV.²³⁶⁹ Kazaa BV launched the first of the three services (the Kazaa service) on July 28, 2000 by publicly releasing its FastTrack software on its web site.²³⁷⁰ The FastTrack software interacted with Kazaa BV's server side software to enable Kazaa users to connect their computers to one or more central computer servers controlled and maintained by Kazaa BV.²³⁷¹ After the central server registered, identified, and logged in the user, the Kazaa service connected the user to a "SuperNode." A SuperNode is a computer with a high-bandwidth connection that is operated by another user already connected to the service. After a user connected to a SuperNode, these "local search hubs" compiled an index of digital files being offered by the user for downloading by other service users. The FastTrack software also enabled users to search for and import preexisting libraries of music files (such as libraries that users built using Napster) to make them available through the service. In response to a search request, the SuperNode reviewed its own index of files and, if necessary, the indices maintained by other SuperNodes. It then displayed the search results to the user to permit the user to download any files displayed by the search.²³⁷² Hence the index of files available at any point in time were distributed throughout various SuperNode computers maintained by the users of the network, not Kazaa BV.

Any Kazaa service user could become a SuperNode by choosing that option in the FastTrack software, and users were encouraged to do so. Kazaa BV's central servers maintained communications with all SuperNodes and assisted in administering the Kazaa service.²³⁷³ The role of Kazaa BV's central servers in the operation of the service was a key basis upon which the plaintiffs asserted contributory and vicarious copyright liability. The Kazaa service continuously monitored its thousands of users to keep track of when they logged on and off. As soon as a user logged on, that user's music files were inventoried and added to the distributed database, and when the user logged off, that user's files were eliminated from the database.²³⁷⁴ Communications on the service between its users' computers and its central servers, between the user and a SuperNode, between SuperNodes and the central servers, and between and among SuperNodes were all encrypted using a scheme controlled by Kazaa BV.²³⁷⁵ According to the complaint, Kazaa BV created the connection between the user who had selected a music file for copying and the user who was offering the selected file. "Thus, all users need to do is select

²³⁶⁹ Class Action Complaint for Copyright Infringement, Leiber v. Consumer Empowerment, Civ. No. 01-09923 (C.D. Cal. Nov. 19, 2001) ¶¶ 25-26.

²³⁷⁰ Id. ¶ 27.

²³⁷¹ Id. ¶ 31.

²³⁷² Id. ¶ 32.

²³⁷³ Id. ¶ 33.

²³⁷⁴ Id. ¶ 34.

²³⁷⁵ Id. ¶ 38.

the file they want and it automatically downloads – *i.e.*, copies and saves – to their individual computer hard drive. [Kazaa BV] makes the entire transaction possible.”²³⁷⁶

The StreamCast and Grokster services operated in a very similar fashion. Initially, both StreamCast and Grokster used the FastTrack software. After the lawsuits were filed, StreamCast switched to use of the open standard Gnutella technology and developed its own software known as “Morpheus” based on that technology. Also after initiation of the lawsuits, the operation of the Kazaa system passed from Kazaa BV to Sharman Networks.²³⁷⁷ A news article reported on May 23, 2002 that Kazaa BV was no longer able to afford defending the lawsuit and that it would accept a default judgment, and that the attorney for StreamCast Networks was withdrawing from the case because StreamCast also could not afford the cost of the litigation.²³⁷⁸

In July of 2002, the federal district court ruled that the plaintiffs could expand their U.S. lawsuit to include Sharman Networks, which had assumed distribution of the Kazaa file-swapping software.²³⁷⁹ In January of 2003, the court rejected a jurisdictional challenge brought by Sharman Networks, ruling that Sharman Networks could be sued in California since the Kazaa software had been downloaded and used by millions of Californians.²³⁸⁰ Approximately one week later, Sharman Networks filed antitrust and copyright misuse counterclaims against the plaintiffs.²³⁸¹

The plaintiffs and defendants StreamCast and Grokster filed cross motions for summary judgment with regard to contributory and vicarious copyright infringement. On April 25, 2003, the court granted summary judgment in favor of StreamCast and Grokster on both theories. The court noted that its order applied only to the then current versions of Grokster’s and StreamCast’s products and services, and did not reach the question of whether either defendant was liable for damages from prior versions of their software or from other past activities.²³⁸²

²³⁷⁶ *Id.* ¶ 37. An internal RIAA memorandum, which both outlines the RIAA’s legal theories against the Kazaa service and gives further technical detail on how it functions, may be found at www.dotcomscoop.com/article.php?sid=39 (available as of Jan. 6, 2002).

²³⁷⁷ *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp. 2d 1029, 1032 & n. 2 (C.D. Cal. 2003).

²³⁷⁸ John Borland, “Kazaa, Morpheus Legal Case Collapsing” (May 22, 2002), available as of May 23, 2002 at <http://news.com.com/2102-1023-920557.html>. The article further reported that “squabbling between Streamcast and Kazaa BV has badly weakened the defendants’ case.”

²³⁷⁹ John Borland, “Judge OKs Suit Against Kazaa Parent” (July 9, 2002), available as of July 10, 2002 at <http://news.com.com/2102-1023-942533.html>.

²³⁸⁰ Declan McCullagh, “Judge: Kazaa Can Be Sued in U.S.” (Jan. 10, 2003), available as of Jan. 13, 2003 at <http://news.com.com/2102-1023-980274.html>.

²³⁸¹ John Borland, “Kazaa Strikes Back at Hollywood, Labels” (Jan. 27, 2003), available as of Jan. 28, 2003 at <http://news.com.com/2102-1023-982344.html>.

²³⁸² *Grokster*, 259 F. Supp. 2d at 1033. The defendant Sharman Networks was not a party to the motions.

With respect to the issue of contributory liability, the court first noted that it was undisputed that at least some of the individuals using the defendants' software were engaged in direct copyright infringement.²³⁸³ The court then turned to an analysis of the two prongs of contributory liability for such direct infringements, knowledge of the infringing activity and material contribution thereto.

In one of the most significant aspects of the ruling, the court held that mere constructive knowledge is not sufficient for contributory liability, but rather the defendant must have actual knowledge of specific infringing acts at the time the infringement occurs. Citing the Ninth Circuit's decision in the Napster case, the court ruled that "defendants are liable for contributory infringement only if they (1) have specific knowledge of infringement at a time at which they contribute to the infringement, and (2) fail to act upon that information."²³⁸⁴ This requirement of specific, actual knowledge seems contrary to the courts' rulings in the Aimster case, discussed in Section III.C.2(c)(3) above, and in the Ellison and Perfect 10 v. Cybernet Ventures cases, discussed in Sections III.C.2(e) and (f) below, that constructive knowledge is sufficient for contributory infringement on the part of a service provider. In addition, the Ninth Circuit's ruling in Napster requiring actual knowledge of specific infringing files, invoked by the Ninth Circuit in its ruling on appeal of the district court's decision in this case, was repudiated by the Supreme Court in its Grokster decision, analyzed in detail below in Section III.C.2(c)(5) below.

The plaintiffs argued that the StreamCast and Grokster defendants had knowledge of the infringing acts because the plaintiffs had sent the defendants thousands of notices regarding alleged infringement. The court held, however, that "notices of infringing conduct are irrelevant if they arrive when Defendants do nothing to facilitate, and cannot do anything to stop, the alleged infringement," as was the case here since the infringing activity took place only after the defendants had distributed their software and, as elaborated under the material contribution prong, they were not in a position to stop the infringing activity.²³⁸⁵

Citing to the Supreme Court's Sony case, the court further ruled that mere distribution of a device that the defendants had general knowledge could be used to commit infringement was insufficient to impose contributory liability, so long as the device was capable of substantial noninfringing uses. The court noted several substantial noninfringing uses for the defendants' software, including distributing movie trailers, free songs or other non-copyrighted work, sharing the works of Shakespeare, and sharing other content for which distribution is authorized.²³⁸⁶

Turning to the material contribution prong, the court ruled that neither StreamCast nor Grokster had materially contributed to the infringing acts of users of their software. The court first noted that the Ninth Circuit found liability in the Napster case because Napster did more

²³⁸³ Id. at 1034.

²³⁸⁴ Id. at 1036 (citing A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1021 (9th Cir. 2001)).

²³⁸⁵ Grokster, 259 F. Supp. 2d at 1037.

²³⁸⁶ Id. at 1035.

than distribute client software – it also hosted a central list of files available on each user’s computer and “thus served as the axis of the file-sharing network’s wheel.”²³⁸⁷ Here, “the critical question is whether Grokster and StreamCast do anything, aside from distributing software, to actively facilitate – or whether they could do anything to stop – their users’ infringing activity.”²³⁸⁸

With respect to Grokster, the court noted that Grokster did not have access to the source code of the FastTrack client software application, and its primary ability to affect its users’ experience was the ability to configure a “start page” in the software and to provide advertising automatically retrieved by the software. An individual node using the FastTrack software automatically self-selected its own supernode status, and utilized a preset list of “root supernodes,” each of which functioned principally to connect users to the network by directing them to active supernodes.²³⁸⁹ “While Grokster may briefly have had some control over a root supernode, Plaintiffs do not dispute that Grokster no longer operates such a supernode. Thus, the technical process of locating and connecting to a supernode – and the FastTrack network – currently occurs essentially independently of Defendant Grokster.”²³⁹⁰ The transfer of files among users was accomplished without any information being transmitted to or through any computers owned or controlled by Grokster.²³⁹¹

With respect to StreamCast, the court noted that the Gnutella technology on which StreamCast was based was a “true” peer-to-peer network that was even more decentralized than FastTrack. Users connected to the Gnutella network by contacting another user who was already connected. The initial connection was usually performed automatically after the user’s computer contacted one of many publicly available directories of those currently connected to the Gnutella network. Instead of using supernodes, search requests on the Gnutella network were passed from user to user until a match was found or the search request expired.²³⁹²

Accordingly, the court concluded that, unlike Napster, neither StreamCast nor Grokster provided the “site and facilities” for direct infringement. Users connected to their respective networks, selected files to share, sent searches, and downloaded files, all without material involvement of the defendants.²³⁹³ “If either Defendant closed their doors and deactivated all computers within their control, users of their products could continue sharing files with little or

²³⁸⁷ Id. at 1039.

²³⁸⁸ Id.

²³⁸⁹ Id. at 1040.

²³⁹⁰ Id. Primary root supernodes on the FastTrack network were operated by Kazaa BV and Sharman Networks. Id. at 1040 n.6.

²³⁹¹ Id. at 1040.

²³⁹² Id. at 1041.

²³⁹³ Id.

no interruption.”²³⁹⁴ The defendants therefore did not provide sufficient material contribution to the infringing acts of users to be liable as contributory infringers.²³⁹⁵

An analysis of the court’s rulings with respect to vicarious liability may be found in Section III.C.3(f) below.²³⁹⁶

On appeal, the Ninth Circuit affirmed.²³⁹⁷ Turning first to the knowledge prong of contributory infringement, the Ninth Circuit noted that any examination of contributory copyright infringement must be guided by the seminal Sony case, under which it is sufficient to defeat a claim of contributory infringement if the defendant shows that its product is capable of substantial or commercially significant noninfringing uses.²³⁹⁸ The court noted that, based on Sony, it had held in the first appeal in the Napster case that if substantial noninfringing use was shown, the copyright owner would be required to show that the defendant had reasonable knowledge of specific infringing files:

Thus, in order to analyze the required element of knowledge of infringement, we must first determine what level of knowledge to require. If the product at issue is not capable of substantial or commercially significant noninfringing uses, then the copyright owner need only show that the defendant had constructive knowledge of the infringement. On the other hand, if the product at issue *is* capable of substantial or commercially significant noninfringing uses, then the copyright owner must demonstrate that the defendant had reasonable knowledge of specific infringing files and failed to act on that knowledge to prevent infringement.²³⁹⁹

Thus, the Ninth Circuit in effect read the Sony case as essentially nothing more than a gloss on the knowledge prong of contributory liability (and therefore inapplicable to vicarious liability), rather than an independent defense to any secondary copyright liability based upon the sale and distribution of technology that is capable of substantial noninfringing uses. The Ninth Circuit further noted that Judge Posner had, in the Aimster case discussed in Section III.C.2(c)(3)

²³⁹⁴ Id.

²³⁹⁵ Id. at 1043. Nor did the provision of technical assistance to their users constitute a material contribution to infringement, because the technical assistance was rendered only after the alleged infringements took place, was routine and non-specific in nature. Id. at 1042.

²³⁹⁶ In January of 2004, the district court ruled that Sharman Networks could pursue claims against the record labels and Hollywood studios for copyright infringement and breach of contract based on allegations that, in their effort to find people sharing files illegally, the labels and studios used unauthorized and unlicensed versions of the Kazaa software to monitor users of the network. Sharman Networks also claimed that the labels breached the software license agreement by sending instant message warnings and bogus files through the network. Jon Healy, “Kazaa Owner Cleared to Sue Record Labels, Movie Studios” (Jan. 23, 2004), available as of Jan. 23, 2004 at www.latimes.com/technology/la-fi-kazaa23jan23,1,2476555.story.

²³⁹⁷ Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 380 F.3d 1154 (9th Cir. 2004).

²³⁹⁸ Id. at 1160-61.

²³⁹⁹ Id. at 1161.

above, read Sony's substantial noninfringing use standard differently by looking at how "probable" the noninfringing uses of a product are. The Ninth Circuit stated that it simply did not read Sony as narrowly as Judge Posner did.²⁴⁰⁰

Because there was no genuine issue of material fact that there were substantial noninfringing uses of the defendants' software, the court concluded that the "reasonable knowledge of specific infringement" requirement was to be applied, and turned to an analysis of whether the copyright owners had raised sufficient genuine issues of material fact to satisfy that higher standard. The Ninth Circuit agreed with the district court that the plaintiffs' notices of infringement were irrelevant to the knowledge prong because they arrived when the defendants did nothing to facilitate, and could not do anything to stop, the alleged infringement of the specific copyrighted content.²⁴⁰¹ The court emphasized the great import of the software design to its holding. Unlike the Napster case, in which Napster maintained a centralized set of servers with an index of available files, no central index was maintained by the defendants' software. Accordingly, even if the defendants were to close their doors and deactivate all their computers, users of their products could continue sharing files with little interruption.²⁴⁰²

Turning to the material contribution prong, the Ninth Circuit agreed with the district court's conclusion that the defendants did not provide the "site and facilities" for infringement because the defendants did not provide file storage or index maintenance on their computers, nor did the defendants have the ability to suspend user accounts.²⁴⁰³ "Rather, it is the users of the software who, by connecting to each other over the internet, create the network and provide the access. 'Failure' to alter software located on another's computer is simply not akin to the failure to delete a filename from one's own computer, to the failure to cancel the registration name and password of a particular user from one's user list, or to the failure to make modifications to software on one's own computer."²⁴⁰⁴

The court also found that the defendants had not materially contributed to the infringement in any other manner. StreamCast maintained an XML file from which user software periodically retrieves parameters, including the addresses of web sites where lists of active users were maintained. The owner of the FastTrack software, Sharman, maintained root nodes containing lists of currently active supernodes to which users could connect. Both defendants also communicated with users incidentally, but not to facilitate infringement. The court found all

²⁴⁰⁰ Id. at 1162 n.9.

²⁴⁰¹ Id. at 1162.

²⁴⁰² Id. at 1163.

²⁴⁰³ Id.

²⁴⁰⁴ Id. at 1163-64.

of these activities too incidental to any direct copyright infringement to constitute material contribution. Accordingly, the defendants were not liable for contributory infringement.²⁴⁰⁵

On appeal, the Supreme Court vacated the Ninth Circuit's decision, rejecting much of its analysis, and remanded the case for further proceedings. The Supreme Court's decision is analyzed in detail in the next subsection below. In November of 2005, in view of the Supreme Court's decision, Grokster agreed to shut down its operations entirely to settle the lawsuits against it. The settlement banned Grokster from participating directly or indirectly in the theft of copyrighted files and required the company to stop giving away its software. Grokster's web site was changed to display a message that said, "There are legal services for downloading music and movies. This service is not one of them."²⁴⁰⁶

Subsequent to the Supreme Court's decision, Grokster settled with the plaintiffs for \$50 million and a permanent injunction,²⁴⁰⁷ and Sharman Networks settled with the plaintiffs for \$115 million and agreed to launch a "legitimate" service.²⁴⁰⁸

International Lawsuits Against the Kazaa Service. Lawsuits were also filed in the Netherlands against the operator of the Kazaa service. On Nov. 29, 2001, an Amsterdam court ordered the service to block customers from trading illegal files by Dec. 13, 2001 or face fines of \$45,000 per day.²⁴⁰⁹ On Jan. 17, 2002, Kazaa suspended downloads of the FastTrack software pending a further decision from the Dutch court.²⁴¹⁰ In late Jan. 2002, Kazaa BV sold its Kazaa.com web site to an Australian firm, Sharman Networks Limited, which then resumed operation of the file-swapping service.²⁴¹¹ In December of 2003, the Dutch Supreme Court affirmed a ruling of the Court of Appeals in Amsterdam that reversed the ruling of the lower court, finding that Kazaa could not be liable for the copyright infringements committed by users

²⁴⁰⁵ *Id.* at 1164. The court noted that the copyright owners had also sought relief based on previous versions of the defendants' software, which contained significant, and perhaps crucial, differences from the software at issue on appeal. The Ninth Circuit noted that it was expressing no opinion as to those issues. *Id.* at 1166.

²⁴⁰⁶ Ted Bridis, "Grokster Downloading Service Shuts Down" (Nov. 7, 2005), available as of Nov. 7, 2005 at <http://news.tmcnet.com/news/2005/nov/1201939.htm>.

²⁴⁰⁷ "Grokster Settles, Streamcast Fights" (Nov. 8, 2005), available as of July 27, 2006 at www.marketingvox.com/archives/2005/11/08/grokster_settles_streamcast_fights/.

²⁴⁰⁸ "Kazaa to Settle File-Share Lawsuits" (July 28, 2006), available as of July 28, 2006 at <http://www.mercurynews.com/mld/mercurynews/business/technology/15143252.htm>. Kazaa also subsequently settled with the music publishers. "Music Publishers Say Kazaa Deal Reached" (Oct. 31, 2006), available as of Nov. 1, 2006 at www.washingtonpost.com/wp-dyn/content/article/2006/10/31/AR2006103100953.htm.

²⁴⁰⁹ Jasper Koning, "Kazaa Plays On Despite Threat of Fines" (Dec. 20, 2001), available as of Jan. 6, 2002 at <http://news.cnet.com/news/0-1005-200-8245314.html>.

²⁴¹⁰ Brad King, "Kazaa Halts Download Distribution" (Jan. 18, 2002), available as of Jan. 18, 2002 at www.wired.com/news/mp3/0,1285,49831,00.html.

²⁴¹¹ Associated Press, "Kazaa Still Up Despite Orders" (Jan. 31, 2002), available as of Feb. 10, 2002 at www.wired.com/news/mp3/0,1285,50165,00.html.

of its software because the Kazaa service did not require centralized servers, as did the Napster service, and the software was capable of sharing many types of files other than audio files and was in fact being used for noninfringing uses.²⁴¹² In December of 2005, Sharman Networks cut off Australians' access to the web site from which the Kazaa file swapping software could be downloaded in order to comply with orders from Australia's Federal Court. Sharman Networks also warned existing Australian users that use of the software was not permitted in Australia, pending an appeal.²⁴¹³

(5) The Supreme Court's Grokster Decision

In one of the most significant copyright decisions since the Sony case, the Supreme Court vacated the Ninth Circuit's ruling in the Grokster case and remanded it for further proceedings. In its decision, taking inspiration again from the patent law, as it had in the Sony case, the Supreme Court introduced inducement liability for the first time into U.S. copyright law. The Court largely sidestepped, however, the opportunity to clarify a number of open questions about the scope of contributory liability and the Sony defense, with respect to many of which the Ninth Circuit and the Seventh Circuit had issued conflicting rulings in the Grokster and Aimster cases, respectively.

Open Issues Going Into the Appeal. In order to best understand the scope of the Supreme Court's decision – both what it decided and the issues it left open – it is useful to begin by noting the issues of secondary liability with respect to which the Ninth Circuit (in its Napster and Grokster decisions) and the Seventh Circuit (in its Aimster decision) had issued contrary rulings before the appeal to the Supreme Court. From the analyses of these cases in earlier sections²⁴¹⁴ it is apparent that the two Circuits differed in their interpretation of Sony on at least the following dimensions:

- What types of secondary liability the Sony defense applies to: contributory liability only (Ninth Circuit) versus both contributory and vicarious liability (Seventh Circuit).
- How the Sony defense should be interpreted: as merely a gloss on the type of knowledge required for contributory liability (Ninth Circuit) versus a cost/benefit analysis of the infringing and noninfringing uses of a system to determine whether contributory liability should be imposed (Seventh Circuit).
- What triggers the Sony defense: mere capability of substantial noninfringing uses of the technology at issue (Ninth Circuit) versus "principal," actual uses (Seventh Circuit).

²⁴¹² "Kazaa Software Does Not Violate Dutch Copyright Law, High Court Rules," *BNA's Electronic Commerce & Law Report* (Jan. 7, 2004) at 11.

²⁴¹³ Ian Ferguson, "Sharman Cuts Off Kazaa Downloads in Australia" (Dec. 5, 2005), available as of Dec. 6, 2005 at www.news.com.com/2100-1027_3-5983455.html.

²⁴¹⁴ See Sections III.C.2(c)(1) & (4) (Napster and Grokster, respectively) and III.C.2(c)(4) (Aimster).

- Whether Sony imposes a duty to redesign technology to avoid or reduce infringing uses: no (Ninth Circuit) versus yes if not disproportionately costly to do so (Seventh Circuit).

These contrary rulings from the Circuits, together with the petitioners' and respondents' briefs and a host of amicus briefs, presented a number of questions that the Supreme Court could have resolved through this case:

- Does Sony afford an independent, stand-alone immunity to secondary copyright liability based upon the sale and distribution of technology that is capable of substantial noninfringing uses, or is it merely a gloss on the knowledge prong of contributory liability?
- More generally, does the Sony defense apply to both contributory and vicarious liability, or only to contributory liability?
- If the Sony defense is an independent immunity, what is its relationship to the traditional doctrines of secondary liability?
- With respect to noninfringing uses of a technology, do merely potential uses count, or only actual uses?
- Is a cost/benefit analysis required to determine whether the Sony immunity should apply?
- Is there any difference between "substantial" and "commercially significant" noninfringing uses and which is the operative test for triggering the Sony immunity (the Supreme Court used both phrases in its Sony opinion in immediately contiguous sentences without elucidating whether it meant any difference between the two phrases, and if so, which standard should govern)?
- Must the distributor of a technology that can be used for infringing uses redesign its product to reduce or eliminate infringing uses in order to avoid secondary liability for them?

In their briefs on appeal, the petitioners urged the following principal positions with respect to these questions:

- That a court should examine the "primary" actual uses of a technology, not merely the potential or theoretical uses, to determine whether its distribution should qualify for immunity from liability under the Sony doctrine;
- That, by analogy to the inducement doctrine of patent law, the defendant's subjective intent with respect to how the technology would or should be used should be examined to determine liability;

- That a cost/benefit analysis as explicated in the Aimster case should always be required to determine whether the Sony immunity is available for a technology;
- That Sony affords a defense only to contributory liability, and not to vicarious liability;
- That one should examine, under the financial benefit prong of the vicarious liability test, whether the defendant's business model is substantially predicated on infringement; and
- That the control prong of vicarious liability should be deemed satisfied where the defendant has failed to exercise control or refused to implement readily available mechanisms to reduce or prevent infringement.

As explicated below, the Supreme Court did not resolve most of the questions identified above, nor did it directly accept any of the positions advocated by the petitioners, at least in the strong form in which they were urged on the Court. Instead, the Court adjudicated the case on its newly introduced doctrine of copyright inducement liability. The Court articulated a standard for inducement liability, noted the kinds of behavior that might give rise to such liability, and remanded the case for further proceedings under the new standard. In the process, the Court's opinion not only left open most of the questions noted above, but gave rise to a number of new questions about the scope of inducement liability that will have to be resolved by the lower courts in future decisions in which inducement liability is invoked by the plaintiff.

The New Doctrine of Inducement Liability. Justice Souter, writing a 9-0 opinion for a unanimous Court, stated the principal question to be decided as "under what circumstances the distributor of a product capable of both lawful and unlawful use is liable for acts of copyright infringement by third parties using the product."²⁴¹⁵ The Court answered this question by formally introducing inducement liability for the first time into U.S. copyright law. To do so, the Court analogized to patent law, as it had in the Sony case:

For the same reasons that *Sony* took the staple-article doctrine of patent law as a model for its copyright safe-harbor rule, the inducement rule, too, is a sensible one for copyright. We adopt it here, holding that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.²⁴¹⁶

This test of inducement liability examines the intent or objective of the distributor of a product or technology that can be used to infringe. Where the distributor has shown "by clear expression or other affirmative steps" that it has an intent or object to foster infringement, there can be liability for inducement. The Court's rule grew out of its exegesis of Sony as a case about

²⁴¹⁵ Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 918-19 (2005).

²⁴¹⁶ Id. at 936-37.

“imputed intent.”²⁴¹⁷ Specifically, Justice Souter noted that “*Sony* barred secondary liability based on presuming or imputing intent to cause infringement solely from the design or distribution of a product capable of substantial lawful use, which the distributor knows is in fact used for infringement.”²⁴¹⁸ Note that Justice Souter used a new phrase (“capable of substantial lawful use”) that is different from each of the alternative two phrases used in *Sony* – “capable of substantial noninfringing uses” and “capable of commercially significant noninfringing uses” – against which a technology or product must be measured for the *Sony* immunity to apply. He did not state, however, whether the new phrase was intended to have a different meaning from either of the phrases used in *Sony*, or to subsume those two phrases into a single moniker.

It is unclear from the majority opinion whether the inducement doctrine is meant to form a third basis for secondary liability, in addition to the traditional contributory and vicarious liability doctrines, or whether the Court intended it to be merely one species of contributory liability. At one point in the opinion, Justice Souter stated, “One infringes contributorily by intentionally inducing or encouraging direct infringement ... and infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it.”²⁴¹⁹ This sentence suggests that intentional inducement is but one species of contributory infringement (or an alternative reading is that contributory liability is defined *solely* as intentionally inducing or encouraging direct infringement), as distinct from vicarious liability. And Justice Souter’s interpretation of *Sony* as a case “about ... imputed intent”²⁴²⁰ reinforces this notion, since intent is the primary issue for copyright inducement liability as set forth by the Court. Yet Justice Breyer’s concurring opinion implies that the inducement doctrine is a new basis for liability distinct from contributory and vicarious liability, for he notes that the Court’s opinion should further deter infringement “by adding a weapon to the copyright holder’s legal arsenal.”²⁴²¹ Justice Ginsburg’s concurring opinion contains a similar inference in her statement that on the record before the Court, *Grokster* and *StreamCast* could be liable “not only for actively inducing copyright infringement,” but “alternatively” for contributory infringement.²⁴²²

Despite the ambiguity in the opinion, it seems to be the better view that the inducement doctrine should be seen as a separate basis for secondary liability distinct from that of the

²⁴¹⁷ *Id.* at 934.

²⁴¹⁸ *Id.* at 933. Justice Souter noted that inferred intent, based solely on the distribution of a product with knowledge that it would be used for some infringing purposes, was the only intent at issue in *Sony* because the record contained “no evidence of stated or indicated intent to promote infringing uses” on the part of Sony. *Id.* at 931.

²⁴¹⁹ *Id.* at 930.

²⁴²⁰ *Id.* at 934. Alternatively, it could reinforce the notion that the Supreme Court intended to redefine contributory liability solely in terms of intentional inducement. Since *Sony* was the leading Supreme Court case on contributory infringement at the time of the *Grokster* opinion, reinterpreting *Sony* as a case about imputed *intent*, rather than imputed *knowledge*, could signal a move by the Supreme Court to reinterpret contributory liability entirely in terms of intent.

²⁴²¹ *Id.* at 957.

²⁴²² *Id.* at 942.

traditional contributory and vicarious liability doctrines. In addition to the fact that Justice Breyer reads it that way in his concurrence, Justice Souter notes that Sony, although it forbade imputing culpable intent as a matter of law from the characteristics or uses of a distributed product, was never meant to foreclose rules of “fault-based liability derived from the common law.”²⁴²³ The traditional doctrine of contributory infringement, as articulated by the courts before the Grokster opinion, was not grounded on a concept of “fault,” thereby suggesting that the inducement doctrine and its associated notion of “fault” is something new. That notion of “fault” is to be found under the inducement doctrine in proof of intent to promote unlawful behavior, coupled with concrete steps taken to act out that intent.²⁴²⁴ In addition, the kinds of evidence the Court notes as relevant to intent and inducement liability is different from the kinds of evidence courts had usually considered for contributory liability before the Grokster decision.²⁴²⁵

The Required Threshold of Showing of Unlawful Intent. From the majority opinion, it appears that the threshold of showing required to prove an unlawful intent to induce infringement will be rather high, so as to “leave[] breathing room for innovation and a vigorous commerce” founded on new technological products:²⁴²⁶

[M]ere knowledge of infringing potential or of actual infringing uses would not be enough here to subject a distributor to liability. Nor would ordinary acts incident to product distribution, such as offering customers technical support or product updates, support liability in themselves. The inducement rule, instead, premises liability on purposeful, culpable expression and conduct, and thus does nothing to compromise legitimate commerce or discourage innovation having a lawful promise.²⁴²⁷

On the other hand, inducement liability is not necessarily limited to encouragement of specific consumers to engage in infringing acts. “It is not only that encouraging a particular

²⁴²³ Id. at 934-35.

²⁴²⁴ The Court noted that the staple article of commerce doctrine in general, and the Sony case in particular, “absolves the equivocal conduct of selling an item with substantial lawful as well as unlawful uses, and limits liability to instances of more acute fault than the mere understanding that some of one’s products will be misused.” Id. at 932-33.

²⁴²⁵ The doctrines of contributory and inducement liability are clearly separate doctrines in the patent law, for they are embodied in separate statutory sections. 35 U.S.C. § 271(b) sets forth inducement liability: “Whoever actively induces infringement of a patent shall be liable as an infringer.” 35 U.S.C. § 271(c) sets forth contributory liability: “Whoever offers to sell or sells within the United States or imports into the United States a component of a patented machine, manufacture, combination or composition, or a material or apparatus for use in practicing a patented process, constituting a material part of the invention, knowing the same to be especially made or especially adapted for use in an infringement of such patent, and not a staple article or commodity of commerce suitable for substantial noninfringing use, shall be liable as a contributory infringer.” Treating inducement and contributory liability as separate doctrines in the copyright law would therefore afford a natural parallel to the patent law, to which the Court analogized in both Sony and Grokster.

²⁴²⁶ Grokster, 545 U.S. at 933.

²⁴²⁷ Id. at 937 (emphasis added).

consumer to infringe a copyright can give rise to secondary liability for the infringement that results. Inducement liability goes beyond that, and the distribution of a product can itself give rise to liability where evidence shows that the distributor intended and encouraged the product to be used to infringe. In such a case, the culpable act is not merely the encouragement of infringement but also the distribution of the tool intended for infringing use.”²⁴²⁸

The Ninth Circuit’s Error. Based on its exegesis of Sony and the rule of inducement liability, the Court noted that the Ninth Circuit had erred in its understanding of secondary liability and the boundaries placed on it by Sony. Specifically, the Ninth Circuit in its Grokster opinion had read Sony’s limitation to mean “that whenever a product is capable of substantial lawful use, the producer can never be held contributorily liable for third parties’ infringing use of it; it read the rule as being this broad, even when an actual purpose to cause infringing use is shown by evidence independent of design and distribution of the product, unless the distributors had ‘specific knowledge of infringement at a time at which they contributed to the infringement, and failed to act upon that information.’”²⁴²⁹ The Court found that the Ninth Circuit had, by this error, converted the case “from one about liability resting on imputed intent to one about liability on any theory.”²⁴³⁰ The Ninth Circuit’s failure to consider an inducement basis for liability, and its affirmance of summary judgment for the defendants, was therefore sufficient grounds for reversal.²⁴³¹ Accordingly, the Court found it unnecessary “to add a more quantified description of the point of balance between protection and commerce when liability rests solely on distribution with knowledge that unlawful use will occur”²⁴³² – in other words, to further explicate what “substantial” or “commercially significant” means as applied to the quantum of noninfringing uses required for Sony’s immunity against imputed intent to apply.

Types of Evidence Relevant to Unlawful Intent. What kinds of evidence will be sufficient to prove an unlawful intent or object to induce or foster infringement? The Court noted the classic examples of “advertising an infringing use or instructing how to engage in an infringing use.”²⁴³³ With respect to the case at bar, the Court noted much in the record that could be used to establish an intent to encourage infringement on the part of the defendants. The Court found three features of this evidence particularly notable:

Targeting Known Demand for Infringing Activity. First, both Grokster and StreamCast showed themselves to be aiming to satisfy a known source of demand for copyright infringement

²⁴²⁸ Id. at 940 n.13. Although the Court does not address the issue, this language may suggest that, where a defendant has established a clear purpose to promote infringement through use of a product it distributes, injunctive relief can extend beyond the affirmative inducing acts and encompass distribution of the product itself.

²⁴²⁹ Id. at 934 (quoting Grokster, 380 F.3d at 1162 (9th Cir. 2004)).

²⁴³⁰ 545U.S. at 934.

²⁴³¹ Id.

²⁴³² Id.

²⁴³³ Id. at 946.

– the market comprising former Napster users.²⁴³⁴ StreamCast’s internal company communications and advertising designs were aimed at Napster users. One ad mockup, for example, stated, “When the lights went off at Napster ... where did the users go?”²⁴³⁵ An internal email from a company executive stated, “We have put this network in place so that when Napster pulls the plug on their free service ... or if the Court orders them shut down prior to that ... we will be positioned to capture the flood of their 32 million users that will be actively looking for an alternative.”²⁴³⁶ Significantly, the Court noted that whether these internal messages or ads were ever communicated to the public did not disqualify them as valid evidence of inducement, because they tended to establish the subjective purpose in the minds of the defendants, particularly when coupled with other evidence of concrete actions taken by the defendants.²⁴³⁷ StreamCast and Grokster both distributed an “OpenNap” program, which was a Napster-compatible program for file sharing. Grokster distributed an electronic newsletter containing links to articles promoting its software’s ability to access popular copyrighted music. The Court also noted that even Grokster’s name was an apparent derivative of Napster.²⁴³⁸ Finally, both companies responded affirmatively to requests for help in locating and playing copyrighted materials.²⁴³⁹

Absence of Effort to Reduce Infringing Activity. Second, the evidence of unlawful objective was given added significance by the fact that neither company attempted to develop filtering tools or other mechanisms to diminish the infringing activity using their software.²⁴⁴⁰ In one of the most significant footnotes in the opinion, the Court stated that, absent other evidence of intent, there is no general duty to redesign a product to reduce or avoid infringement: “Of course, in the absence of other evidence of intent, a court would be unable to find contributory infringement liability merely based on a failure to take affirmative steps to prevent infringement, if the device otherwise was capable of substantial noninfringing uses. Such a holding would tread too close to the *Sony* safe harbor.”²⁴⁴¹ However, in this case, the Court believed that, given the very strong other evidence of intent to induce infringement, the failure to develop filtering tools underscored the defendants’ intentional facilitation of their

²⁴³⁴ Id. at 939.

²⁴³⁵ Id. at 938. Another read, “Napster Inc. has announced that it will soon begin charging you a fee. That’s if the courts don’t order it shut down first. What will you do to get around it?” Id. at 925.

²⁴³⁶ Id. at 924-25. StreamCast delivered a press kit containing press articles about its potential to capture former Napster users, and it introduced itself to some potential advertisers as a company “which is similar to what Napster was.” Id. at 924. StreamCast also planned to flaunt the illegal uses of its software; its chief technology officer averred that “the goal is to get in trouble with the law and get sued. It’s the best way to get in the news.” Id. at 925.

²⁴³⁷ Id. at 938. “Even if these advertisements were not released to the public and do not show encouragement to infringe, they illuminate StreamCast’s purposes.” Id. at 925 n.7.

²⁴³⁸ Id. at 924, 938.

²⁴³⁹ Id. at 938.

²⁴⁴⁰ Id. at 939.

²⁴⁴¹ Id. at 939 n.12.

users' infringement.²⁴⁴² Moreover, the record established that the defendants had responded to questions from their users about how to play infringing movies they had downloaded.²⁴⁴³

Gains Proportional to Infringing Activity. Third, StreamCast's and Grokster's monetary gains were proportional to the volume of infringement by their users. Because both companies made money by selling advertising space directed to the screens of users, the more their software was used, the more ads that would be sent out and the greater their advertising revenues. The companies therefore had incentive to encourage high volume use, which the record showed was infringing.²⁴⁴⁴ Again, the Court noted that "[t]his evidence alone would not justify an inference of unlawful intent, but viewed in the context of the entire record its import is clear."²⁴⁴⁵

Summary of Significant Aspects of the Court's Ruling. Based on the preceding analysis, the following key aspects of the majority opinion can be summarized:

- A defendant can be liable for inducing copyright infringement where the defendant takes acts or other affirmative steps with the subjective intent to promote infringement. The Court has, however, established a high standard of proof for demonstrating the required subjective intent to induce infringement, for its opinion uses language requiring "clear expression or other affirmative steps taken to foster infringement,"²⁴⁴⁶ "purposeful, culpable expression and conduct,"²⁴⁴⁷ and "a patently illegal objective."²⁴⁴⁸ The purpose of this high standard is so as not to "compromise legitimate commerce or discourage innovation having a lawful purpose."²⁴⁴⁹
- Inducement liability cannot be based on the mere "characteristics" of a product, including its functional capability for use for infringing purposes, or on the mere "knowledge that it may be put to infringing uses."²⁴⁵⁰ Instead, for inducement liability, "statements or actions directed to promoting infringement" through use of the technology are required.²⁴⁵¹ Thus, the Court's rule for inducement liability focuses on subjective purpose of the defendant rather than the technology itself. Two vendors of

²⁴⁴² Id. at 393.

²⁴⁴³ Id. at 923.

²⁴⁴⁴ Id. at 940.

²⁴⁴⁵ Id. Thus, "the business models employed by Grokster and StreamCast confirm that their principal object was use of their software to download copyrighted works." Id. at 926.

²⁴⁴⁶ Id. at 937.

²⁴⁴⁷ Id.

²⁴⁴⁸ Id. at 941.

²⁴⁴⁹ Id. at 937.

²⁴⁵⁰ Id. at 935.

²⁴⁵¹ Id.

the same technology could therefore have different liability depending upon their actions and the intent behind them.

- Even where a distributed technology is used by some to commit infringement, the vendor of that technology can engage in ordinary acts incident to product distribution, such as offering customers technical support or product updates, and those acts, in themselves, will not establish inducement liability.²⁴⁵²
- The basic immunity of the Sony case remains intact. Sony continues to “bar[] secondary liability based on presuming or imputing intent to cause infringement solely from the design or distribution of a product capable of substantial lawful use, which the distributor knows is in fact used for infringement.”²⁴⁵³
- In judging the subjective intent of a defendant accused of inducing infringement, a court may look at evidence of internal communications (whether or not released to the public or potential users), the business model of the defendant and whether it is predicated on infringement, product naming, advertising and press kits, customer support activities in response to specific questions about how to use the technology for infringing acts, targeting of users who are known to be committing or likely to commit infringing acts using the technology in question, whether the defendant has taken steps to reduce or eliminate use of its technology for infringement, and whether the defendant’s gain is proportional to infringing volume.
- In the absence of other evidence of intent, mere failure to design or redesign a technology to avoid or reduce infringing uses, by itself, cannot form the basis of liability, if the technology is otherwise capable of substantial noninfringing uses.²⁴⁵⁴ Where there is other evidence of purpose, however, failure to take steps to prevent infringing uses of a technology can reinforce an inference of subjective intent to induce infringement.

The Court left open a host of questions with respect to the issue of product design and infringement avoidance, which the lower courts will be left to work out:

- What threshold showing of intent must be made before the failure to design a product to reduce or avoid infringement becomes relevant to show culpable purpose to encourage infringement? The Court’s opinion generally requires “clear expression or other affirmative steps” to promote infringement. Must the plaintiff therefore show a “clear expression” of purpose or “affirmative steps” taken through other evidence before the evidence of failure to design becomes even relevant? Or is a lesser quantum of other evidence sufficient to trigger the relevancy of failure to design evidence, which can then be aggregated with such other evidence to make a showing of “clear expression”? If a

²⁴⁵² Id. at 937.

²⁴⁵³ Id. at 933.

²⁴⁵⁴ Id. at 939 n.12.

lesser quantum of other evidence is sufficient, what is that quantum?²⁴⁵⁵ And must such other evidence be direct evidence, or may it be circumstantial evidence?

- Once evidence of failure to design to avoid infringement becomes relevant, what substantive standard governs the extent to which the product must be designed to avoid or reduce infringement? Presumably some kind of reasonableness standard will govern that looks to both the state of the art of technology that could be deployed in the design to reduce infringement, as well as the costs and benefits of that technology.
- Does the copyright holder itself have a duty to reduce or prevent infringement of its copyrighted material by deploying technology (such as DRM technology) to protect it at the time of distribution? If so, how is the burden to deploy technological means to reduce infringement to be allocated between the copyright holder and the distributor of the products or services that are ultimately used to commit infringement?
- Can a defendant use evidence of affirmative steps it took to prevent infringement as a defense to inducement liability?
- Monetary gain from infringing activity does not by itself justify an inference of unlawful intent. But where there is other strong evidence of unlawful intent, gain that is proportional to infringing activity can be reinforcing evidence of intent.²⁴⁵⁶ Similar questions as those discussed in the preceding bullets arise with respect to the threshold showing of intent through other evidence that must be made before evidence of monetary gain from infringing activity is relevant. Also unknown is the substantive standard governing what kinds of monetary gain will be cognizable as evidence of intent to promote infringement, and how directly tied to the infringing activity such monetary gain must be.

One can expect that the doctrine of inducement will take on a jurisprudential life of its own, with attendant uncertainty as to standards and outcomes as further judicial development takes place. The focus on subjective intent and the business model of the defendant will likely make summary judgment more difficult to obtain in inducement cases than in other secondary liability cases. Finally, one can expect that the written record relating to development and

²⁴⁵⁵ The inducement rule set up by the Court in Grokster appears to differ a bit from the active inducement rule in patent law. Some patent cases, most notably Oak Industries, Inc. v. Zenith Electronics Corp., 726 F. Supp. 1525 (N.D. Ill. 1989), distinguish between an affirmative act directed toward encouraging or promoting infringement, and the distinct element of intent to induce, which can be proved by evidence not only of affirmative acts but also design omissions. By contrast, the Grokster opinion requires that intent be shown by “clear expression or other affirmative steps taken to foster to infringement.” Unlike the patent law, then, intent cannot be established through acts of design omission alone. See Matthew Brown et al., “Secondary Liability for Inducing Copyright Infringement After MGM v. Grokster: Infringement-Prevention and Product Design,” *Journal of Internet Law*, Dec. 2005, at 21, 25.

²⁴⁵⁶ Grokster, 545 U.S. at 940.

promotion of a technology, including purely internal communications, will be crucial to the issue of intent and therefore the focus of discovery and litigation in inducement cases.

The Concurring Opinions – Disagreement About the Scope of the Sony Safe Harbor.

Despite the urging of the petitioners, the majority opinion found it unnecessary to provide “a more quantified description” of what level of noninfringing uses are required to qualify as “substantial” or “commercially significant” within the meaning of Sony. Six of the justices, however, in two concurring opinions, joined this issue and advocated significantly different positions.

The first concurring opinion was authored by Justice Ginsburg and joined by Chief Justice Rehnquist and Justice Kennedy. Justice Ginsburg noted that, in addition to liability under the inducement doctrine articulated by the majority, one could be liable under traditional contributory infringement principles for distributing a product that users use to infringe copyrights, if the product is not capable of “substantial” or “commercially significant” uses.²⁴⁵⁷ Without choosing between, or articulating any difference between, the two phrases “substantial” and “commercially significant,” she elaborated on her understanding of what those phrases in Sony mean collectively.

Although not stating so explicitly, Justice Ginsburg’s opinion seems based on two key interpretations of the Sony safe harbor: (i) that it requires a court to focus more on actual uses of a product, or those that are concretely likely to develop over time, rather than merely potential uses, and (ii) that one should balance the relative numbers of infringing and noninfringing uses, and not merely the absolute number of noninfringing uses.

With respect to the first principle, Justice Ginsburg expressed the belief that, unlike in Sony, there had been no finding of fair use and “little beyond anecdotal evidence of noninfringing uses.”²⁴⁵⁸ She noted that the district court’s conclusion of substantial noninfringing uses rested almost entirely on a collection of declarations submitted by Grokster and StreamCast, and that review of those declarations showed a collection of mostly anecdotal evidence, sometimes obtained second-hand, of authorized copyrighted works or public domain works available online and shared through peer-to-peer networks, and general statements about the benefits of peer-to-peer technology.²⁴⁵⁹ She concluded that the declarations did not support summary judgment in the face of evidence proffered by the plaintiffs of “overwhelming use of Grokster’s and StreamCast’s software for infringement”²⁴⁶⁰ – clearly focusing on the current, actual uses of the software. Nor did she see a realistic possibility that concrete noninfringing uses were likely to develop over time. “Fairly appraised, the evidence was insufficient to

²⁴⁵⁷ Id. at 942 (Ginsburg, J., concurring).

²⁴⁵⁸ Id. at 945.

²⁴⁵⁹ Id. at 946.

²⁴⁶⁰ Id. at 947.

demonstrate, beyond genuine debate, a reasonable prospect that substantial or commercially significant noninfringing uses were likely to develop over time.”²⁴⁶¹

Concerning the second principle, Justice Ginsburg stated, “Even if the absolute number of noninfringing files copied using the Grokster and StreamCast software is large, it does not follow that the products are therefore put to substantial noninfringing uses and are thus immune from liability. The number of noninfringing copies may be reflective of, and dwarfed by, the huge total volume of files shared.”²⁴⁶²

The second concurring opinion, authored by Justice Breyer and joined by Justices Stevens and O’Connor, expressly disagreed with Justice Ginsburg’s opinion and articulated a very different understanding of the Sony safe harbor. Justice Breyer began his analysis by noting how low a number of actual authorized uses were required in Sony to qualify as “substantial.” Specifically, the record showed that of all the taping actually done by Sony’s customers, only around 9% was of the sort the Court referred to as authorized, yet the Court found the magnitude of authorized programming was “significant.”²⁴⁶³ Justice Breyer noted that the Sony Court had concluded from this evidence that rights owners had authorized duplication of their copyrighted programs “in significant enough numbers to create a *substantial* market for a noninfringing use” of the VCR.²⁴⁶⁴ By using the key word “substantial,” the Sony Court had concluded that 9% authorized uses alone constituted a sufficient basis for rejecting the imposition of secondary liability. Justice Breyer then concluded that, when measured against the evidence of authorized use present in Sony, the evidence before the Court in the Grokster case should be sufficient to pass the test of Sony. Specifically, the plaintiffs’ evidence showed 75% of current files available on Grokster as infringing and 15% likely infringing. That left approximately 10% of files that were apparently noninfringing, a figure very similar to the 9% of authorized uses of the VCR the Court faced in Sony.²⁴⁶⁵

In addition, Justice Breyer noted that Sony’s standard also incorporates the word “capable” with respect to noninfringing uses, and concluded “that a figure like 10%, if fixed for all time, might well prove insufficient, but that such a figure serves as an adequate foundation where there is a reasonable prospect of expanded legitimate uses over time.”²⁴⁶⁶ He found that the record revealed a significant future market for noninfringing uses of peer-to-peer software like Grokster’s, and the combination of such foreseeable development, together with an estimated 10% of existing noninfringing material, is sufficient to meet Sony’s standard.²⁴⁶⁷

²⁴⁶¹ Id. at 948

²⁴⁶² Id.

²⁴⁶³ Id. at 950-51.

²⁴⁶⁴ Id. at 951 (quoting Sony, 464 U.S. at 447 n.28) (emphasis added by Justice Breyer).

²⁴⁶⁵ Grokster, 545 U.S. at 952.

²⁴⁶⁶ Id.

²⁴⁶⁷ Id. at 954.

Justice Breyer then reviewed the appellate decisions construing Sony and noted that only one – the Seventh Circuit’s Aimster decision – had interpreted Sony more strictly than he would do.²⁴⁶⁸ Based on a review of those appellate decisions, he concluded that Sony establishes “that the law will not impose copyright liability upon the distributors of dual-use technologies (who do not themselves engage in unauthorized copying) unless the product in question will be used *almost exclusively* to infringe copyrights (or unless they actively induced infringements as we today describe).”²⁴⁶⁹

Justice Breyer lauded this interpretation of Sony as encouraging technical innovation by providing “entrepreneurs with needed assurance that they will be shielded from copyright liability as they bring valuable new technologies to market.”²⁴⁷⁰ It does so in the following ways.²⁴⁷¹

- The Sony rule, as so interpreted, is clear, and allows those who develop new products that are capable of substantial noninfringing uses to know, *ex ante*, that distribution of their product will not yield massive monetary liability.
- It is strongly technology protecting, sheltering a product unless it will be used almost exclusively to infringe.
- It is forward looking, and does not confine the safe harbor to a static snapshot of a product’s current uses, but rather looks to uses of which the product is capable.²⁴⁷²
- It is mindful of the limitations facing judges where matters of technology are concerned, since judges have no specialized technical ability to answer questions about present or future technological feasibility or commercial viability where technology professionals, engineers, and venture capitalists may radically disagree and where answers may differ depending upon whether one focuses upon the time of product development or the time of distribution.

Justice Breyer concluded that a modified Sony rule as urged by the petitioners or as interpreted by Justice Ginsburg would significantly chill technological development, as innovators would have no way to predict how courts would weigh the respective values of infringing and noninfringing uses, determine the efficiency and advisability of technological changes or assess a product’s potential future markets.²⁴⁷³

²⁴⁶⁸ Id. at 955.

²⁴⁶⁹ Id. 957.

²⁴⁷⁰ Id.

²⁴⁷¹ See id. at 957-58.

²⁴⁷² Justice Breyer interpreted the word “capable” as used in Sony to refer “to a plausible, not simply a theoretical, likelihood that such uses will come to pass, and that fact anchors Sony in practical reality.” Id. at 958.

²⁴⁷³ Id. at 959-60.

Justice Breyer concluded his opinion with the question of whether a modified Sony rule would yield a positive copyright impact that would outweigh any technology-related loss. Although he acknowledged that a more intrusive Sony test would generally provide greater revenue security for copyright holders, he found it harder to conclude that the gains to copyright holders would exceed the losses to innovation. “For one thing, the law disfavors equating the two different kinds of gain and loss; rather, it leans in favor of protecting technology.”²⁴⁷⁴ In addition, since Sony has been the law for quite some time, there should be a serious burden on copyright holders to show a need for a more strict interpretation of the current rules. Justice Breyer concluded that a strong demonstrated need for interpreting the Sony standard more strictly had not been shown and that the Court should maintain Sony, reading it as he had interpreted it.²⁴⁷⁵

Issues Left Open by the Supreme Court. The Supreme Court’s opinion left open a host of unanswered questions concerning secondary liability and the scope of the Sony immunity. Among them are the following:

- Whether there is any substantive difference between the phrases “capable of substantial noninfringing uses” and “capable of commercially significant noninfringing uses” as used in Sony. None of the majority opinion or the two concurrences expressly analyzes a difference, and all seem to treat the phrases as interchangeable. However, given that all justices agreed that the Sony standard need not be revisited as part of the Court’s disposition of the case, and given that Justice Souter introduced yet a third phrase in the majority opinion – “capable of substantial lawful use” – the issue was not definitively resolved by the case.
- Whether Sony requires consideration of the relative balance of the infringing uses against the noninfringing uses of a technology. Justice Ginsburg’s concurrence seems to require such a balance, whereas Justice Breyer’s concurrence does not. The majority opinion does not reach the issue.
- Whether Sony requires some minimal threshold of noninfringing uses, and if so, what that threshold is. The wide split in conclusions from the record in the Grokster case expressed in the concurring opinions illustrate how unsettled this question was among the members of the Court that decided Grokster. Moreover, three justices did not express an opinion of any kind on the issue.
- What “capable of” means in the Sony test. Both concurrences seem to reject a meaning of purely theoretical uses. However, Justice Ginsburg’s concurrence focuses much more on the actual uses of a product, whereas Justice Breyer’s concurrence evidences more of a willingness to look to future legitimate uses that might be precluded by a strict interpretation of the Sony safe harbor. Stated differently, Justice Ginsburg’s concurrence

²⁴⁷⁴ Id. at 960.

²⁴⁷⁵ Id. at 960-66.

appears predisposed to favor the copyright holders rights, whereas Justice Breyer's concurrence is predisposed to favor technological innovation.

- Whether the Sony immunity applies to both contributory and vicarious liability, or only to contributory liability. Justice Souter's majority opinion does not address vicarious liability at all: "Because we resolve the case based on an inducement theory, there is no need to analyze separately MGM's vicarious liability theory."²⁴⁷⁶
- What level of active encouragement will be sufficient to find inducement in less egregious cases. Related questions include (i) the meaning of "clear expression" of intent and "purposeful, culpable expression and conduct," and (ii) if there is little "expressive" evidence of purpose, what kinds of acts or omissions will qualify as "other affirmative steps taken to foster infringement."
- At what point in time the defendant's "intent" is to be measured – at the time of original design of the technology, at the time of distribution, at some other time?
- Whether the defendant must merely intend to induce the acts that give rise to infringement, or intend to cause infringement itself. For example, what happens if the defendant had a good faith belief at the time of product design or promotion that the intended acts were fair use, but they are later judged infringing? Must the belief be objectively reasonable?
- Under what circumstances failure to design or redesign a product to avoid or reduce infringement can be used as proof of intent to induce infringement, and when a vendor of technology has an obligation to redesign in order to avoid inducement liability. As analyzed above, there are a host of questions left unanswered by the Court's opinion with respect to the issue of design to avoid infringement.
- Whether the Seventh Circuit's approach to the Sony safe harbor in the Aimster case is correct or not. None of the three opinions in Grokster expressly address whether the Aimster approach erred in various aspects. The majority opinion cites the Aimster case only for the factual proposition that it may be impossible to enforce rights in a protected work effectively against all direct infringers, making the only practical alternative going against the distributor of the copying device for secondary liability.²⁴⁷⁷ Justice Ginsburg's concurring opinion merely notes the conflict between the Aimster and Napster decisions and states only that all members of the Court agree that the Ninth Circuit misapplied Sony, at least to the extent it read that decision to limit secondary liability to a "hardly-ever category."²⁴⁷⁸ Justice Breyer's concurring opinion cites Aimster only for the proposition that there is but a single appellate decision to date interpreting Sony more

²⁴⁷⁶ Id. at 931 n.9 (Souter, J.).

²⁴⁷⁷ Id. at 929-30.

²⁴⁷⁸ Id. at 944 n.1 (Ginsburg, J., concurring).

strictly than Justice Breyer would.²⁴⁷⁹ Nevertheless, it seems that, to the extent the Aimster decision suggests that failure to affirmatively prevent infringing uses could by itself, without other evidence of unlawful intent, subject a defendant to liability, it is plainly inconsistent with the Grokster majority opinion.²⁴⁸⁰ In addition, Aimster's general cost/benefit balancing approach to the Sony safe harbor may not survive the majority opinion either.²⁴⁸¹

Although the Grokster case is one of the most important copyright decisions to come out of the Supreme Court, it clearly left much work to be done by the lower courts, and perhaps the Supreme Court itself in future copyright decisions, to work out the boundaries of the copyright inducement doctrine and the Sony safe harbor.

(6) The Grokster Decision on Remand

(i) The Ruling on Liability

Defendant Grokster settled with the plaintiffs shortly after the Supreme Court's decision. On remand from the Supreme Court, the district court granted the plaintiffs' motion for summary judgment as to liability of defendants StreamCast and Sharman for inducing copyright infringement.²⁴⁸² Not surprisingly, the district court's ruling essentially tracked the Supreme Court's analysis, which had strongly presaged the ultimate outcome of the case.²⁴⁸³ By and large, the district court's opinion did little more than elaborate factually on the various bases the Supreme Court had identified in its opinion upon which the defendants could be held liable under the inducement doctrine.

The district court may, however, have put one important gloss on the Supreme Court's legal rulings that may represent an extension of the scope of inducement liability. Specifically, StreamCast argued that a defendant could be found liable under the inducement doctrine only if it: (1) for the purpose of inducing infringement, (2) took actions beyond distributing infringement

²⁴⁷⁹ Id. at 955 (Breyer, J., concurring).

²⁴⁸⁰ "Of course, in the absence of other evidence of intent, a court would be unable to find contributory infringement liability merely based on a failure to take affirmative steps to prevent infringement, if the device otherwise was capable of substantial noninfringing uses. Such a holding would tread too close to the Sony safe harbor." Id. at 939 n.12 (Souter, J.).

²⁴⁸¹ See Mitchell Zimmerman, "Does Aimster Survive Grokster," *Cyberspace Lawyer*, Dec. 2005, at 1 (noting that Aimster insisted that "balancing of costs and benefits is necessary," even in cases "in which substantial noninfringing uses, present or prospective, are demonstrated, whereas Grokster says instead that "the [Sony] doctrine absolves the equivocal conduct of selling an item with substantial lawful as well as unlawful uses ..."). Mr. Zimmerman's article notes several other ways in which the Grokster majority opinion may *sub silentio* disapprove of Aimster.

²⁴⁸² Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, 454 F. Supp. 2d 966 (C.D. Cal. 2006).

²⁴⁸³ Indeed, the district court noted in its opinion after reviewing all the evidence that "in Grokster the Supreme Court had hinted that summary judgment should be granted for Plaintiffs after reviewing much of the same evidence." Id. at 992.

enabling technology, and (3) which actually resulted in specific instances of infringement. In StreamCast's view, even if it distributed peer-to-peer software with the intent for it to be used for infringement, liability would not attach unless it took further actions, such as offering instructions on infringing use, that actually caused specific acts of infringement. StreamCast devoted much energy to arguing that the plaintiffs had failed to prove the second and third elements of its proposed test.²⁴⁸⁴

The district court rejected StreamCast's argument, finding it contrary to the following language from the Supreme Court's decision:

It is not only that encouraging a particular consumer to infringe a copyright can give rise to secondary liability for the infringement that results. Inducement liability goes beyond that, and the distribution of a product can itself give rise to liability where evidence shows that the distributor intended and encouraged the product to be used to infringe. In such a case, the culpable conduct is not merely the encouragement of infringement but also the distribution of the tool intended for infringing use.²⁴⁸⁵

From this passage, the district court went on to conclude, "Thus, Plaintiffs need not prove that StreamCast undertook specific actions, beyond product distribution, that caused specific acts of infringement. Instead, Plaintiffs need prove only that StreamCast distributed the product with the intent to encourage infringement."²⁴⁸⁶ Although not entirely clear, it appears that in the district court's view, as long as a defendant has a subjective intent to encourage infringement, the mere distribution of a product that is used by others to commit infringement is sufficient to make the distributor of the product secondarily liable. Such a rule, however, appears to be inconsistent with the Supreme Court's ruling. In the passage quoted by the district court, the Supreme Court stated that "distribution of a product can itself give rise to liability where evidence shows that the distributor intended *and encouraged the product to be used to infringe*."²⁴⁸⁷ The use of the conjunctive "and" followed by a requirement of encouraging a product to be used to infringe suggests that the Supreme Court did not view distribution of a product alone, coupled with a subjective intent on the part of the distributor to encourage infringement, would be sufficient for inducement liability. Rather, the distributor must in addition take actions that encourage the product to be used to infringe. Although the facts of the case, as elaborated below, seem sufficient to establish StreamCast's liability under either rule, the district court's articulation of the rule seems broader than, and therefore contrary to, the Supreme Court's Grokster ruling.

²⁴⁸⁴ Id. at 984.

²⁴⁸⁵ Id. at 984-85 (quoting Grokster, 545 U.S. at 940 n.13).

²⁴⁸⁶ 454 F. Supp. 2d at 985.

²⁴⁸⁷ Grokster, 545 U.S. at 940 n.13 (emphasis added).

In any event, following the outline of the Supreme Court’s analysis, the district court found a sufficient basis for inducement liability on the part of StreamCast based upon the following facts:

-- StreamCast’s software was used overwhelmingly for infringement: A study by the plaintiffs’ experts showed that 87.33% of the files offered for distribution on the Morpheus network, and that almost 97% of the files actually requested for downloading, were infringing or highly likely to be infringing. The district court noted that, while infringing use by third parties was not by itself evidence of StreamCast’s intent, the staggering scale of infringement made it more likely that StreamCast condoned illegal use and provided a backdrop against which all of StreamCast’s actions had to be assessed.²⁴⁸⁸

-- StreamCast targeted Napster users: The district court found uncontroverted evidence, including internal communications, promotional efforts, advertising designs, and actual advertisements, establishing that StreamCast purposefully targeted Napster users, not merely to market to them, but to convert them into StreamCast users by offering them the same file-sharing service that Napster had itself offered.²⁴⁸⁹

-- StreamCast assisted infringing uses: StreamCast provided users with technical assistance for playback of copyrighted content, in one instance suggesting to a user who complained about the paucity of music from Elvis and Muddy Waters that he upload copyrighted content for sharing.²⁴⁹⁰

-- StreamCast ensured its technology had infringing capabilities: Among other things, the district court cited to evidence that, before deciding to license FastTrack technology for Morpheus, StreamCast’s chairman evaluated FastTrack by searching for Garth Brooks songs on the FastTrack network. While Morpheus was in beta testing, StreamCast employees identified the insufficient quantity of popular copyrighted content on the network as an important problem, and many StreamCast employees tested the software’s infringing capabilities by downloading copyrighted tracks. The Morpheus interface contained a search category for “Top 40” songs that were almost invariably copyrighted. And the court noted that StreamCast took active steps to protect illegal file trading from the enforcement efforts of copyright holders and deployed encryption technology so that the plaintiffs could not see what files were being transferred through Morpheus.²⁴⁹¹

-- StreamCast’s business model depended on massive infringing use: The record established that StreamCast knew its business model depended on massive infringing use, and acted to grow its business accordingly. StreamCast’s CTO testified that StreamCast’s objective in advertising to Napster users was to increase the number of users by increasing the amount of

²⁴⁸⁸ 454 F. Supp. 2d at 985.

²⁴⁸⁹ *Id.* at 985-86.

²⁴⁹⁰ *Id.* at 986-87.

²⁴⁹¹ *Id.* at 987-88.

file sharing, since the more files that were physically available, the more users would come. The company tracked its progress after launch by tracking the number of files that were available for sharing, particularly as against those available for sharing through Napster.²⁴⁹²

-- StreamCast took no meaningful affirmative steps to prevent infringement: Although noting that secondary liability could not be premised on failure to prevent infringing use alone, the district court noted the Supreme Court's holding that a defendant's failure to do so can indicate an intent to facilitate infringement.²⁴⁹³ Based on this, the district court ruled, "By implication, although StreamCast is not required to prevent all the harm that is facilitated by the technology, it must at least make a good faith attempt to mitigate the massive infringement facilitated by its technology."²⁴⁹⁴ The district court noted at least two technologies that StreamCast could have used to implement a system to filter out copyrighted content from the Morpheus network – acoustic fingerprinting using unique digital signatures for each music file for identification and metadata that describes the properties of a file, such as song title and artist name. With respect to the latter, the court noted that Morpheus executed file searches on the basis of metadata such as song names, and contained a feature that, if activated by the user, would filter out pornographic content on the basis of file name. The plaintiffs argued that the technology behind the pornographic filter could easily have been reconfigured to filter out copyrighted content.²⁴⁹⁵

StreamCast countered that metadata filtering would be burdensome and overbroad, as it would block all files that shared common words in metadata, even if the file was not copyrighted. StreamCast also argued that, with regard to FastTrack-based versions of Morpheus, it did not have the ability to directly modify the FastTrack source code, which the licensor controlled, to implement filtering.²⁴⁹⁶ The court noted that, based on the foregoing, a jury could reasonably agree with StreamCast that copyright filtering would not work perfectly and implementing it would negatively impact usability.²⁴⁹⁷ However, the court ruled that "the ultimate question ... is to examine StreamCast's intent. Even if filtering technology does not work perfectly and contains negative side effects on usability, the fact that a defendant fails to make some effort to mitigate abusive use of its technology may still support an inference of intent to encourage infringement."²⁴⁹⁸

The court further noted that StreamCast saw its resistance to filtering as a competitive advantage, citing testimony of StreamCast's chairman that if Napster were forced to filter, StreamCast would take all of Napster's users. StreamCast was unreceptive when it was

²⁴⁹² Id. at 988-89.

²⁴⁹³ Id. at 989.

²⁴⁹⁴ Id.

²⁴⁹⁵ Id. at 989-90.

²⁴⁹⁶ Id. at 990.

²⁴⁹⁷ Id.

²⁴⁹⁸ Id.

approached by GraceNote, a company that had worked with Napster on a way to use acoustic fingerprinting technology to identify copyrighted music and pay copyright holders.²⁴⁹⁹

Finally, the court ruled, although not in the context of a DMCA safe harbor defense asserted by StreamCast, that StreamCast's blocking of users from its network in response to requests from copyright holders was insufficient to absolve it from liability:

This Court recognizes that StreamCast blocked certain users from its network when asked to do so by copyright holders. However, its effort was half-hearted at best. As described above, StreamCast used encryption technology to defeat Plaintiffs' monitoring efforts. Moreover, blocking users was not very effective because a user could simply create a new username to re-enter the network under a different identity. StreamCast had the capability of automatically blocking these users on a rolling basis, but expressly decided not to do so.²⁵⁰⁰

Based on these factual findings, the court concluded that "evidence of StreamCast's objective of promoting infringement is overwhelming" and granted summary judgment of liability for inducement on the part of StreamCast.²⁵⁰¹

(ii) The Permanent Injunction

In a subsequent opinion, the district court considered the plaintiffs' proposal for a very broad permanent injunction against StreamCast.²⁵⁰² The court noted that, under the Supreme Court's decision in the eBay case,²⁵⁰³ to be entitled to a permanent injunction on their copyrights, the plaintiffs were required to satisfy the traditional four part test for injunctive relief of irreparable harm, inadequate remedies at law, a balance of hardships in their favor, and that the public interest would not be disserved by an injunction.²⁵⁰⁴ The court first turned to whether, having established infringement, the plaintiffs were entitled to a presumption of irreparable harm, and concluded that a presumption of irreparable harm no longer inures to a plaintiff after eBay in a permanent injunction case.²⁵⁰⁵ Nevertheless, the court found that irreparable harm had been established for two reasons. First, Streamcast had and would

²⁴⁹⁹ Id. at 991.

²⁵⁰⁰ Id. at 992. The court did not elaborate on how StreamCast could have automatically blocked users on a "rolling basis."

²⁵⁰¹ Id. at 992, 999.

²⁵⁰² Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 2007 U.S. Dist. LEXIS 79726 (C.D. Cal. Oct. 16, 2007).

²⁵⁰³ eBay, Inc. v. MercExchange, L.L.C., 126 S. Ct. 1837 (2006).

²⁵⁰⁴ Grokster, 2007 U.S. Dist. LEXIS at *30.

²⁵⁰⁵ Id. at *38-40. The court noted significant division among the existing post eBay decisions concerning whether the traditional presumption of irreparable harm in a preliminary injunction context flowing from a showing of likelihood of success on the merits also failed to survive eBay. The court noted that, although the law was muddled and the Ninth Circuit had not yet spoken on the point post eBay, the better view is that the presumption probably did not survive eBay in a preliminary injunction context. Id. at *43-49.

continue to induce far more infringement than it could ever possibly redress with damages. Second, absent an injunction, a substantial number of the plaintiffs' copyrighted works would continue to be made available for unending infringement outside of the Morpheus system and software, effectively eviscerating the plaintiffs' ability to protect their property rights.²⁵⁰⁶

The court found that the plaintiffs had no adequate remedy at law because a statutory recovery for those infringements induced through the Morpheus system would not compensate the plaintiffs when those same files were subsequently shared outside the Morpheus system. The balance of hardships tipped in the plaintiffs' favor because StreamCast would likely engage in further inducement in the absence of a permanent injunction. Finally, an injunction would serve the public interest since it would protect the plaintiffs' copyrights against increased infringement.²⁵⁰⁷

Turning to the scope of the injunction, the court first ruled that the scope should not extend beyond inducement activities, because inducement was the only form of infringement that StreamCast had been found liable for. Accordingly, the court rejected the plaintiffs' proposed broad wording for the injunction to the extent it would reach activities giving rise to liability solely under contributory or vicarious liability doctrines, although the court noted that the injunction could properly extend to copyrighted works of the plaintiffs whether then in existence or later created.²⁵⁰⁸

The court then turned to the most interesting and significant issue relating to the injunction – whether it should require StreamCast to implement filtering of the plaintiffs' copyrighted works on its system, and if so, to what extent. StreamCast argued that, under Sony, its continued distribution of the Morpheus system and software was legal, even without filtering technology, so long as StreamCast did not engage in any additional actions or statements promoting infringement, because the system and software were capable of substantial non-infringing uses.²⁵⁰⁹ The court rejected this argument, reasoning that under the Supreme Court's Grokster opinion, once acts of encouragement or promotion of infringement through a product or system have taken place, the further distribution of that product or system can be restricted as further acts of inducement:

It is important to recognize that the Supreme Court did not impose any strict timing relationship between specific acts promoting infringements, distribution, and the direct infringements themselves. For a party to be liable for inducement, distribution may begin prior to any promotion of infringement, distribution and promotion can occur at

²⁵⁰⁶ Id. at *57-62. The court ruled it would make no difference to the irreparable harm analysis if Streamcast's inducement was demonstrated to increase the plaintiffs' sales because, as copyright owners, plaintiffs "have the exclusive right to decide when and how their material should be reproduced and/or distributed, regardless of whether their decisions make good business sense." Id. at *63.

²⁵⁰⁷ Id. at *66-73.

²⁵⁰⁸ Id. at *88,-94.

²⁵⁰⁹ Id. at *100.

the same time, and most critically, distribution can follow past promotion. ... As a matter of common sense, a successful inducer will sometimes have no need to repeat the infringing message ad infinitum. This is especially likely to be the case where the product in question is overwhelmingly used for infringing purposes, and requires little or no specialized training to operate. At a certain point, the inducer can simply continue to distribute the product without any additional active encouragement, recognizing that the marketplace will respond in turn.

Thus, once the market has internalized the inducer's promotion of infringement, the resulting infringements should be attributable to that defendant even though he/she no longer chooses to actively promote that message. ... Thus, distribution of a product capable of substantial noninfringing uses, even after the promotion/encouragement of infringement ceases, can by itself constitute inducement.²⁵¹⁰

In view of these principles, the court concluded that the injunction must impose a filtering obligation on StreamCast because an unfiltered Morpheus system and software would necessarily capitalize on and remain inexorably linked to StreamCast's historical efforts to promote infringement.²⁵¹¹ The court rejected, however, the plaintiffs proposal that StreamCast be enjoined from distributing Morpheus or another peer-to-peer network unless and until it had demonstrated to the court's satisfaction that it contained "robust and secure means exhaustively to prevent users from using" the system to infringe.²⁵¹² The court noted that there is no filtering system that could "exhaustively" stop every single potential infringement on a peer-to-peer network, and plaintiffs should not, through a standard that stringent, be effectively given the right to prohibit entirely the distribution of a product having substantial noninfringing uses.²⁵¹³

Instead, the court concluded that it would issue a permanent injunction requiring StreamCast to reduce Morpheus' infringing capabilities, while preserving its core noninfringing functionality, as effectively as possible.²⁵¹⁴ "Streamcast's duties will include, but not necessarily be limited to: (1) a filter as part of future Morpheus software distributed to the public; and (2) steps to encourage end-user upgrades from non-filtered software."²⁵¹⁵ The court noted that cost of such filtering, while a relevant criterion if all else were equal, "is not likely a controlling factor, as the injunction will be designed primarily to protect Plaintiffs' copyrights. The mere fact

²⁵¹⁰ Id. at *106-08.

²⁵¹¹ Id. at *110-11.

²⁵¹² Id. at *112.

²⁵¹³ Id. at *113-14.

²⁵¹⁴ Id. at *115.

²⁵¹⁵ Id. at *115-16.

that an adjudicated infringer may have to expend substantial resources to prevent the consummation of further induced infringements is not a central concern.”²⁵¹⁶

Lastly, the court turned to the issue of whether, and to what extent, the injunction should require notice from the plaintiffs of their copyrighted works in order to trigger StreamCast’s duty to filter those works. The court noted that in the Napster case the Ninth Circuit had imposed notice obligations on the plaintiffs before Napster had a duty to disable access to the offending content on its system.²⁵¹⁷ The court reflected that, although Sony’s knowledge prong is completely irrelevant to whether one can be held liable as a vicarious infringer, the Ninth Circuit had nevertheless, by imposing a notice requirement on the plaintiffs, essentially allowed Sony notice concerns “to creep back into the vicarious infringement analysis for purposes of an injunction.”²⁵¹⁸ Accordingly, although actual notice of specific infringing files and the failure to remove them is not a prerequisite to inducement liability in the first instance, the Ninth Circuit’s Napster ruling informed the court that, like vicarious infringement, notice should be relevant to the injunction against StreamCast.²⁵¹⁹ The court ruled that StreamCast’s duty to filter any particular copyrighted work would commence upon the plaintiffs’ provision of notice in the form of artist-title pair, a certification of ownership, and some evidence that one or more files containing each work was available on the Morpheus system.²⁵²⁰

By order dated Nov. 29, 2007, the court appointed a special master, Andy Johnson-Laird, to assist the court. The court ordered the special master to report on the type of filtering system that should be used (e.g., artist and title matching, hash value digital fingerprinting, and/or acoustical fingerprinting) for the most effectiveness at eliminating the greatest number of infringing works while allowing the core noninfringing uses to continue, and on the most effective way by which StreamCast could encourage current users of legacy software versions to upgrade to a version that possessed the requisite filtering technology.²⁵²¹ “The final Report shall include a comprehensive regimen of the actions StreamCast needs to undertake, the forms of filtering necessary, and the methods for implementation of these tools. Such a Report is to

²⁵¹⁶ Id. at *117.

²⁵¹⁷ Id. at *118-19.

²⁵¹⁸ Id. at *120.

²⁵¹⁹ Id. at *121. The court amplified as follows: “One might argue that Napster’s notice requirement should not be followed in light of the Supreme Court’s Grokster opinion. At one point, the Supreme Court stated that ‘Sony did not displace other theories of secondary liability,’ and is confined to cases involving ‘imputed intent.’ It could reasonably be argued, as a result, that Sony occupies a much less central position in the copyright field than was previously understood. Since Sony cannot preclude vicarious and inducement liability, the doctrine could now be viewed as irrelevant to injunctions aimed at preventing such violations. However, this Court will not read this implication into the Supreme Court’s ruling, nor hold that Napster has been overruled sub silentio on this question.” Id. at *121-22 (citations omitted).

²⁵²⁰ Id. at *123.

²⁵²¹ Order re Appointment of Special Master, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., CV 01-8541 SVW (C.D. Cal. Nov. 29, 2007) at pp. 5-7.

include any details of the filtering, such as how StreamCast can adopt keyword filters, common misspellings, and file extensions into filtering technology.”²⁵²²

(7) The Audiogalaxy Case

On May 24, 2002, various record companies, music publishers and songwriters filed a class action lawsuit against the peer-to-peer filing sharing service Audiogalaxy, alleging liability for contributory and vicarious copyright infringement for facilitating the copying of digital music files over the Internet. The plaintiffs alleged that the Audiogalaxy service was even worse than the Napster system in facilitating infringement, because the Audiogalaxy service allowed users to download entire record albums, cover art, and software.²⁵²³ Less than one month later, on June 17, 2002, the plaintiffs announced a settlement with Audiogalaxy that required the file sharing service to halt the infringement of copyrighted works on its network and allowed, but did not require, the service to employ a “filter-in” system that would not make music available without the consent of the copyright holder. Audiogalaxy also agreed to pay the plaintiffs a substantial sum in settlement.²⁵²⁴

(8) The Hummer Winblad/Bertelsmann Litigation

After Napster filed for bankruptcy, several of the plaintiffs in the Napster litigation brought suit against the venture capital firm Hummer Winblad and the media company Bertelsmann AG, each of which had funded Napster, seeking to hold those defendants secondarily liable for the infringement of the plaintiffs’ works committed through the Napster system. The plaintiffs alleged that by investing in Napster and assuming control of the operation of Napster,²⁵²⁵ the defendants contributorily and vicariously infringed the plaintiffs’ rights. In July of 2004, Judge Patel denied summary judgment motions filed by the defendants, ruling that the plaintiffs’ allegations that Bertelsmann and Hummer Winblad “exercised essentially full operational control over Napster during periods in which Napster remained a conduit for infringing activity” would, if proved, give rise to liability for contributory and vicarious infringement.²⁵²⁶

The defendants subsequently filed motions for summary judgment seeking to limit their liability for copyright infringement to those works that were the subject of notice to Napster, and more narrowly, those works of which Bertelsmann had actual notice, in view of the Ninth Circuit’s rulings in Napster I and Napster II, discussed extensively in Section III.C.2(c)(1) above.

²⁵²² Id. at p. 7.

²⁵²³ “Record Labels, Music Publishers, Songwriters Sue Audiogalaxy; Allege It Is Same as Napster,” *BNA’s Electronic Commerce & Law Report* (June 5, 2002) at 561-62.

²⁵²⁴ “RIAA, NMPA Reach Settlement With Audiogalaxy,” *BNA’s Electronic Commerce & Law Report* (June 26, 2002) at 655.

²⁵²⁵ Hank Berry, a partner at the Hummer Winblad firm, was installed by Hummer Winblad as Napster’s CEO shortly after Hummer Winblad made a substantial venture capital investment in Napster.

²⁵²⁶ UMG Recordings, Inc. v. Bertelsmann AG, 222 F.R.D. 408 (N.D. Cal. 2004).

Judge Patel's opinion of May 2006 denying such motions²⁵²⁷ afforded her an interesting and detailed opportunity to construe some of the more confusing aspects of the Napster I and Napster II cases, as well as to explicate the effect of the Supreme Court's Grokster decision on the Ninth Circuit's rulings and their applicability to Hummer Winblad's and Bertelsmann's secondary liability.

In moving for summary judgment, the defendants argued that the Ninth Circuit's rulings in Napster I and Napster II limited Napster's liability to those works of which Napster had actual notice and which Napster failed to remove from its system. The Plaintiffs disputed the defendants' reading of Napster I, and also argued that Judge Patel's holding in Fonovisa, Inc. v. Napster, Inc.²⁵²⁸ and the Supreme Court's Grokster decision firmly established that actual notice is not required. The defendants argued that the ultimate holding of Napster I, however it might have been called into question by the Grokster case, with respect to the degree of Napster's liability was binding in the instant litigation.²⁵²⁹ To adjudicate the contentions of the plaintiffs and the defendants, Judge Patel revisited the Napster I, Fonovisa v. Napster, and Grokster decisions in detail.

Turning first to the Napster I decision, the court noted that the Ninth Circuit's rulings with respect to the standard of knowledge required – actual versus constructive – were confusing. The Ninth Circuit began its opinion by noting that Napster had both actual and constructive knowledge of direct infringements committed through the Napster system. But then the Ninth Circuit's opinion abruptly shifted when it quoted language from the court's opinion in the Netcom case to the effect that evidence of actual knowledge of specific acts of infringement is required to hold a computer system operator liable for contributory copyright infringement.²⁵³⁰

Judge Patel noted that the Ninth Circuit's discussion of the Netcom case was confusing in several respects. First, the Ninth Circuit's opinion stated at least two formulations of the level of knowledge required for infringement, suggesting alternately that actual knowledge was *required* and that it was *sufficient*. Second, the Ninth Circuit's opinion did not explicitly discuss constructive knowledge as an alternate basis for liability. Judge Patel noted, however, that focusing on the Ninth Circuit's own formulations of the legal standard, and not on the quote from the Netcom decision, it would be possible to read the first half of Napster I as upholding Judge Patel's findings on both actual and constructive knowledge and affirming liability on both bases.²⁵³¹

However, Judge Patel noted that the portion of the Ninth Circuit's opinion modifying the scope of her preliminary injunction presented a second discontinuity in reasoning. The Ninth

²⁵²⁷ In re Napster, Inc. Copyright Litigation, 2006 U.S. Dist. LEXIS 30338 (N.D. Cal. May 17, 2006).

²⁵²⁸ 2002 U.S. Dist. LEXIS 4270 (N.D. Cal. Jan. 28, 2002).

²⁵²⁹ In re Napster, Inc. Copyright Litigation, 2002 U.S. Dist. LEXIS 4270 at *13.

²⁵³⁰ Id. at *14-16.

²⁵³¹ Id. at *19.

Circuit set forth a three factor test defining the boundary of Napster’s contributory liability: Napster could be liable to the extent it (1) received reasonable knowledge of specific infringing files with copyrighted works, (2) knew or should have known that such files were available on the Napster system, and (3) failed to act to prevent viral distribution of the works. The references to “reasonable” knowledge and “should have known” of the availability of infringing files again suggested a constructive knowledge standard.²⁵³²

Nevertheless, the Ninth Circuit went on to formulate guidelines for the narrowing of the injunction. First, the Ninth Circuit placed the burden on the plaintiffs to provide notice to Napster of copyrighted works and files containing such works available on the Napster system. Second, after plaintiffs provided notice, Napster had the duty to disable access to the offending content, as well as the additional burden of policing the system within the limits of the system (i.e., searching the system for similarly named files). Judge Patel found this section of the Ninth Circuit’s opinion to demonstrate the inconsistency in its reasoning. Despite finding that Napster had constructive knowledge based on facts unrelated to specific infringing files, the Ninth Circuit nonetheless in effect limited Napster’s liability to those files of which Napster had actual knowledge.²⁵³³

Judge Patel then summarized her conclusions from the Napster I case as follows:

Whether or not it is supported by clear reasoning, the Ninth Circuit explicitly stated that Napster must have “reasonable knowledge” of specific infringing works before it could be found liable. Plaintiffs attempt to avoid the consequences of the Ninth Circuit’s holding by arguing that the rules used in crafting an injunction are distinct from those used in determining damages. The Ninth Circuit, however, expressly limited Napster’s “liability,” (i.e., the extent of its infringing conduct), according to the “reasonable knowledge” standard before embarking on a discussion of how the injunction should be modified. Although the actual proposed mechanics of the injunction – notice followed by a duty to remove the files – may be narrower than the outer limits of Napster’s liability, there is no doubt that Napster I significantly reduced the scope of Napster’s exposure.²⁵³⁴

Judge Patel then turned to a discussion of her ruling in the Fonovisa decision, in which Napster, moving to dismiss Fonovisa’s complaint, had argued that Napster I added a “notice” requirement for claims of secondary copyright infringement by on-line systems. Judge Patel rejected Napster’s arguments in her 2004 decision in Fonovisa, finding that although Napster I set fairly narrow limits on Napster’s liability, it studiously avoided any clear reshaping of the doctrine of contributory infringement.²⁵³⁵

²⁵³² Id. at *19-20.

²⁵³³ Id. at *20-22.

²⁵³⁴ Id. at *22-23.

²⁵³⁵ Id. at *24.

Judge Patel then observed that her Fonovisa opinion had set forth four points relevant to Hummer Winblad’s and Bertelsmann’s instant motions for summary judgment. First, liability is not necessarily coextensive with injunctive relief or damages, and the required mental state for Napster’s liability remained “reasonable knowledge.” Second, the conduct identified by the Napster I court as infringing use – actual notice followed by a failure to correct – was exemplary and not intended to be an exhaustive list. Under the “reasonable knowledge” standard, other methods of proving actual and constructive knowledge were possible, although Napster I admittedly set the bar for reasonable knowledge quite high. Third, it was significant that Fonovisa considered only a motion to dismiss and not the precise scope of liability. To survive a motion to dismiss, a plaintiff need identify only a specific instance of infringement, whereas the same facts would be inadequate in proving the precise amount of damages. And fourth, Judge Patel had acknowledged in Fonovisa that broader readings of Napster I were possible, but absent a compelling reason to do so, she was unwilling to read more into it than it stated.²⁵³⁶

Judge Patel then turned to an analysis of the Grokster decision. She noted that the Ninth Circuit’s opinion in Grokster had read Napster I more expansively than she had anticipated in Fonovisa, reading Napster I to mean that if a defendant could show that its product was capable of substantial or commercially significant noninfringing uses, then constructive knowledge of the infringement could not be imputed. Judge Patel noted that the Supreme Court rejected the Ninth Circuit’s ruling, and that taken as a whole, the Supreme Court’s decision provided for liability under broader circumstances than those permitted under Napster I. She noted that the evidence stressed by the Supreme Court, particularly the defendants’ advertising and marketing strategies – was strikingly similar to the evidence supporting her finding of constructive knowledge in shaping her original, more sweeping injunction in the Napster case.²⁵³⁷

The defendants argued that the Grokster ruling could not be applied retroactively to the current case to render actionable conduct that conformed to the modified preliminary injunction entered following Napster I, a closed case that was no longer on direct review. Judge Patel rejected this argument, noting that Bertelsmann was a different party than Napster, and the instant action was not the same as the now-closed original Napster lawsuit. Bertelsmann was alleged to be separately liable based on its own control over the operation of the Napster system, even if its liability were factually derivative of the same alleged acts of illegal copying by Napster. Accordingly, the court ruled that the plaintiffs were entitled to pursue recovery under the Grokster theory of liability, which did not require actual or even reasonable knowledge of specific infringing files, as well as under the “reasonable knowledge” standard articulated in Napster I.²⁵³⁸ Accordingly, she denied the defendants’ motion for summary judgment.²⁵³⁹

²⁵³⁶ Id. at *24-27.

²⁵³⁷ Id. at *27-30.

²⁵³⁸ Id. at *31-32.

²⁵³⁹ Id. at *33.

In 2006, while appeals were pending before the Ninth Circuit, Bertelsman and Hummer Winblad reached a settlement with the plaintiffs.²⁵⁴⁰

(9) Arista Records v. Lime Group

(For a discussion of contributory liability in this case, see Section III.C.4(d) below.)

(d) The CoStar Case

In CoStar v. Loopnet,²⁵⁴¹ discussed in detail in Section III.C.6(b)(1)(iii).c below, the court addressed in some detail the knowledge an OSP must have of infringing activity in order to be liable for contributory infringement. In brief summary, the plaintiff argued that once it gave the OSP notice of specific infringements on its system, the OSP was on notice that ongoing infringements were occurring and had a duty to prevent repeat infringements in the future. The court ruled that the amount of policing for future infringements the OSP would be required to do would depend upon the level of knowledge it possessed and the specificity of that knowledge. The court further held that, to prove its claim for contributory infringement, the plaintiff would have to establish that the notice it gave to the OSP comprised at least constructive knowledge of specific infringing activity which the OSP materially contributed to or induced by its alleged failure to halt the activity. There remained too many material factual disputes for the court to decide on summary judgment either that such a level of knowledge did or did not exist or that the OSP's actions in trying to stop the infringement were or were not insufficient to the point of comprising inducement as a matter of law.

(e) Ellison v. Robertson

In Ellison v. Robertson,²⁵⁴² discussed in detail in Section III.C.6(b)(1)(i)b. below, the district court addressed the “reason to know” prong of the knowledge requirement of contributory liability. In that case an individual named Robertson scanned several fictional works written by the plaintiff and posted them onto the Usenet group “alt.binaries.e-book,” a group that was used primarily to exchange pirated and unauthorized digital copies of text material, principally works of fiction by famous authors. AOL, acting as a Usenet peer, hosted the infringing materials on its Usenet server for a period of fourteen days. The plaintiff sought to hold AOL liable for direct, vicarious and contributory copyright infringement.²⁵⁴³

With respect to contributory infringement, the court found that AOL did not have actual knowledge of the infringement until the lawsuit was filed. Although the plaintiff had attempted to notify AOL of the presence of the infringing works via email to AOL's designated copyright

²⁵⁴⁰ Anne Urda, “End in Sight for Hummer Winblad in Napster Saga,” ” *Law360* (Dec. 7, 2006), available as of Dec. 7, 2006 at www.law360.com/articles/14725/end-in-sight-for-hummer-winblad-in-napster-saga.

²⁵⁴¹ 164 F. Supp. 2d 688 (D. Md. 2001), *aff'd*, 373 F.3d 544 (4th Cir. 2004).

²⁵⁴² 189 F. Supp. 2d 1051 (C.D. Cal. 2002).

²⁵⁴³ *Id.* at 1053-54.

agent as listed in the Copyright Office's records, AOL never received the email because AOL had changed its contact email address from "copyright@aol.com" to "aolcopyright@aol.com" in Fall 1999, but waited until April 2000 to notify the Copyright Office of this change. The district court held that, in view of AOL's failure to explain why it delayed in notifying the Copyright Office of its email address change, as well as why it did not make provision for forwarding to the new address emails sent to the old address, a reasonable trier of fact could find that AOL had reason to know that infringing copies of the plaintiff's works were stored on its Usenet servers.²⁵⁴⁴ The Ninth Circuit affirmed this ruling on appeal.²⁵⁴⁵

With respect to the material contribution prong of contributory infringement, AOL argued that as a matter of law, the mere provision of Usenet access was too attenuated from the infringing activity to constitute a material contribution, citing for support by analogy the provisions of Section 512(m) of the DMCA that an OSP need not monitor its system for infringing activity to qualify for the DMCA safe harbors. The district court rejected this argument, citing the Netcom court's holding that providing a service that allows for the automatic distribution of all Usenet postings can constitute a material contribution when the OSP knows or should know of infringing activity on its system and yet continues to aid in the distribution of the infringing material. Accordingly, the district court ruled that the plaintiff had demonstrated triable issues of fact on contributory infringement by AOL.²⁵⁴⁶ The Ninth Circuit also affirmed this ruling on appeal.²⁵⁴⁷

(f) Perfect 10 v. Cybernet Ventures

In Perfect 10, Inc. v. Cybernet Ventures, Inc.,²⁵⁴⁸ the defendant Cybernet was the operator of an "age verification service" that enrolled subscribers, after verifying their age as an adult, to a service that would enable them to gain access for a single monthly fee to a large number of member sites displaying pornographic pictures. All fees paid by subscribers went directly to Cybernet, which on a semi-monthly basis then paid each individual member site a commission based on the site where the subscriber originally signed up for his or her

²⁵⁴⁴ Id. at 1057-58. The court also noted that a trier of fact might conclude that AOL had reason to know of infringement on its system from the fact that another AOL user had called AOL to report a number of infringing books posted on Usenet. The user spoke only to a low-level customer service representative, who advised him to send an email setting forth the details of his complaint. The court stated, "a reasonable trier of fact might conclude that AOL should have transferred Miller to speak with an employee with knowledge of AOL's copyright infringement policies instead of directing him to an email address." Id. at 1058.

²⁵⁴⁵ Ellison v. Robertson, 357 F.3d 1072, 1077 (9th Cir. 2004) ("Because there is evidence indicating that AOL changed its e-mail address in an unreasonable manner and that AOL should have been on notice of infringing activity we conclude that a reasonable trier of fact could find that AOL had reason to know of potentially infringing activity occurring within its USENET network.").

²⁵⁴⁶ Ellison v. Robertson, 189 F. Supp. 2d 1051, 1058-60 (C.D. Cal. 2002).

²⁵⁴⁷ Ellison v. Robertson, 357 F.3d 1072, 1078 (9th Cir. 2004).

²⁵⁴⁸ 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

membership in Cybernet's service.²⁵⁴⁹ Cybernet exercised some control over the content of each of its member sites, requiring that each site contain unique and adequate content, which generally meant at least 30 pictures of sufficient quality to provide value to Cybernet's customers. Cybernet also imposed a zero tolerance child pornography policy on its member sites.²⁵⁵⁰ The court found that Cybernet actively reviewed and directed its affiliated webmasters on the appearance and content of their sites.²⁵⁵¹

The plaintiff, Perfect 10, was the holder of copyright in various photographs of nude women. Perfect 10 claimed to have found more than 10,000 copies of its photographs on approximately 900 websites affiliated with Cybernet.²⁵⁵² Perfect 10 sought to hold Cybernet liable for the unauthorized presence of its photographs on Cybernet's member sites.

On a motion for a preliminary injunction, the court ruled that Perfect 10 had established a strong likelihood of success on its claim of contributory copyright infringement. The court found that Cybernet had knowledge of the infringements because a member for the Association for the Protection of Internet Copyright had contacted Cybernet with approximately 2,000 emails over the course of three or four years, notifying Cybernet of alleged copyright infringement on its system. In addition, Cybernet's site reviewers reviewed every site before allowing the sites to become members of Cybernet's service, and the court found that there was evidence that many sites contained disclaimers to the effect that the site did not hold copyrights for the works on the site.²⁵⁵³ Accordingly, the court ruled that there was "a strong likelihood of success in proving general knowledge of copyright infringement prior to Perfect 10's filing of the complaint" as well as "serious questions as to Cybernet's constructive knowledge of infringement of Perfect 10's copyrights prior to the complaint raised by this general knowledge, Cybernet's review of sites containing Perfect 10 images and the likelihood of those sites containing copyright disclaimers. Further, there appears to be little question that Cybernet has been provided with actual notice of a large number of alleged infringements since June 2001."²⁵⁵⁴

Citing the Fonovisa case,²⁵⁵⁵ the court also concluded that Cybernet had materially contributed to the infringements by providing technical and content advice to its member sites, reviewing those sites, and attempting to control the quality of the product it presented to subscribers as a unified brand.²⁵⁵⁶

²⁵⁴⁹ Id. at 1159.

²⁵⁵⁰ Id. at 1160-61.

²⁵⁵¹ Id. at 1164.

²⁵⁵² Id. at 1162.

²⁵⁵³ Id. at 1169.

²⁵⁵⁴ Id. at 1170 (emphasis in original).

²⁵⁵⁵ Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996).

²⁵⁵⁶ Perfect 10, 213 F. Supp. 2d at 1170.

(g) Perfect 10 v. Visa International

In Perfect 10, Inc. v. Visa International Service Ass'n,²⁵⁵⁷ Perfect 10, owner of the copyrights in pornographic materials, sought to hold various credit card and banking institutions liable for contributory and vicarious infringement for providing financial services to various web sites that Perfect 10 alleged contained infringing copies of its copyrighted materials. The district court granted the defendants' motion to dismiss.

With respect to contributory liability, the defendants did not contest the issue of their knowledge of infringement, but denied that they materially contributed to the infringement. The district court agreed. Unlike the defendant age verification service in Perfect 10, Inc. v. Cybernet Ventures, Inc.,²⁵⁵⁸ which advertised the infringing web sites and paid a commission to a web site whenever someone registered for its services through that particular web site, the court noted that the defendants in the instant case did not promote the web sites that used their services, nor have any content-specific regulations with which merchants must comply before using their services.²⁵⁵⁹

The court rejected Perfect 10's argument that because the defendants provided essential financial services to alleged infringers, they were materially contributing to the infringement. The court noted that the financial services were not essential to the functioning of the allegedly infringing web sites because they could employ intermediate payment services if the defendants terminated their merchant accounts. Furthermore, even if the defendants provided services that materially contributed to the functioning of the web site businesses, there was no factual basis for the allegation that they materially contributed to the alleged *infringing activities* of the web sites. The defendants' ability to process credit cards did not directly assist the allegedly infringing web sites in copying the plaintiffs' works. Accordingly, the court ruled that Perfect 10 had not adequately pled a claim for contributory infringement, although the court granted Perfect 10 leave to amend its complaint to establish a relationship between the financial services provided by the defendants and the alleged infringing activity.²⁵⁶⁰

On appeal, the Ninth Circuit affirmed.²⁵⁶¹ With respect to contributory infringement, the court noted that it need not address the knowledge prong because it found that Perfect 10 had not pled facts sufficient to establish that the defendants induced or materially contributed to the infringing activity.²⁵⁶² With respect to material contribution, the court held that merely continuing to process credit card payments to the infringing web sites despite knowledge of ongoing infringement was insufficient contribution for contributory liability because such

²⁵⁵⁷ 71 U.S.P.Q.2d 1914 (N.D. Cal. 2004), aff'd, 494 F.3d 788 (9th Cir. 2007), cert. denied, 553 U.S. 1079 (2008).

²⁵⁵⁸ 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

²⁵⁵⁹ Perfect 10, Inc. v. Visa International, 71 U.S.P.Q.2d at 1917.

²⁵⁶⁰ Id.

²⁵⁶¹ Perfect 10, Inc. v. Visa International, 494 F.3d 788 (9th Cir. 2007), cert. denied, 553 U.S. 1079 (2008).

²⁵⁶² Id. at 795.

payment services had no direct connection to the actual infringing activities of reproduction or distribution of the plaintiff's copyrighted material. The defendants' services did not assist users in searching for infringing images, nor provide links to them, nor did infringing materials pass through the defendants' payment systems. Although the payment services made it easier for web sites to profit from the infringing activities, this fact was insufficient for contributory liability because the services did not directly assist in the *distribution* of infringing content to Internet users. The court noted that even if users couldn't pay for images with credit cards, infringement could still continue on a large scale because other viable funding mechanisms were available.²⁵⁶³

The court rejected Perfect 10's argument that the defendants' payment services were akin to provision of the site and facilities for infringement analogous to the Fonovisa case. The court noted that the web sites on which the infringing photographs resided were the "site" of the infringement, not the defendants' payment networks. If mere provision of a method of payment could be considered a "facility" of infringement, so too could the provision of computers, of software, and of electricity to the infringing web sites, and such a rule would simply reach too far.²⁵⁶⁴

With respect to inducement, Perfect 10 argued that the Grokster decision was analogous because the defendants induced customers to use their cards to purchase goods and services, and should therefore be held guilty of specifically inducing infringement if the cards were used to purchase images from sites that had stolen content from Perfect 10. The court rejected this argument as insufficient, noting that Perfect 10 had pled no facts suggesting that the defendants had promoted their payment system as a means to infringe, nor had they promoted the purchase of specific infringing goods. Accordingly, the facts as pled evidenced no clear expression of a specific intent to foster infringement, and thus there could be no liability for inducement.²⁵⁶⁵

The court's rulings with respect to vicarious liability are set forth in Section III.C.3.(g) below.

(h) Parker v. Google

In Parker v. Google,²⁵⁶⁶ pro se plaintiff Gordon Parker was the owner of copyright in an e-book titled "29 Reasons Not To Be A Nice Guy." He posted Reason # 6 on USENET. Parker asserted that Google's automatic archiving of this USENET content made Google contributorily liable for copyright infringement because it facilitated users to make unauthorized distributions and copies of his copyrighted material through the "author search" feature on Google's web site. The district court rejected this argument for two reasons. First, Parker failed to allege infringement of a specific copyrighted work in his claim for contributory infringement. And

²⁵⁶³ Id. at 796-797.

²⁵⁶⁴ Id. at 798-800.

²⁵⁶⁵ Id. at 800-02.

²⁵⁶⁶ 422 F. Supp. 2d 492 (E.D. Pa. 2006), aff'd, 2007 U.S. App. LEXIS 16370 (3rd Cir. July 10, 2007).

second, he had failed to allege that Google had requisite knowledge of a third party's infringing activity.²⁵⁶⁷ On appeal, the Third Circuit affirmed in an unpublished opinion on the ground that Parker had failed to allege that Google had the requisite knowledge of a third party's infringing activity.²⁵⁶⁸

(i) MDY Industries v. Blizzard Entertainment

In MDY Industries v. Blizzard Entertainment,²⁵⁶⁹ the defendant distributed bot software called "Glider" that was able to play Blizzard Entertainment's multiplayer online role-playing game known as World of Warcraft (WoW) for its owner while the owner was away from his or her computer, thereby enabling the owner to advance more quickly within WoW than would otherwise be possible. Glider also enabled its user to acquire an inordinate number of game assets, with some users even selling those assets for money in online auction sites. Both the use of bot software to play WoW and the resale of game assets were prohibited by the Terms of Use (TOU) that governed the play of WoW, together with an End User License Agreement (EULA). The EULA and TOU were displayed on a player's computer screen when the game client software was loaded and the player sought online access to Blizzard's game servers. Players were required to agree to the terms of the EULA and TOU before proceeding to play the game. Blizzard alleged that users of WoW were licensees who were permitted to copy the copyrighted game client software only in conformance with the EULA and TOU, and that when users launched WoW using Glider, they exceeded the license in the EULA and TOU and created infringing copies of the game client software. Blizzard sought to hold the defendant contributorily liable for those infringing copies.²⁵⁷⁰

The district court agreed and granted Blizzard summary judgment against the defendant. Citing the Ninth Circuit's decision in MAI Sys. v. Peak Computer, Inc.,²⁵⁷¹ the court ruled that copying of software to RAM constitutes "copying" for purposes of Section 106 of the Copyright Act, and thus if a person is not authorized by the copyright holder through a license or by law (e.g. Section 117) to copy the software to RAM, the person commits copyright infringement by using the software in an unauthorized way.²⁵⁷² The court ruled that the provisions in the EULA and the TOU prohibiting the use of bots and resale of game assets were limitations on the scope of the license, not merely separate contractual covenants. The EULA stated the game client software was distributed solely for use by authorized end users according to the terms of the EULA, and the grant clause in the license was expressly conditioned as being subject to the end user's continuing compliance with the EULA. The license also made clear that, although users were licensed to play WoW and to use the game client software while playing, they were not

²⁵⁶⁷ Id. at 498-99.

²⁵⁶⁸ Parker v. Google, 2007 U.S. App. LEXIS 16370 at *9 (3d Cir. July 10, 2007).

²⁵⁶⁹ 2008 U.S. Dist. LEXIS 53988 (D. Ariz. July 14, 2008).

²⁵⁷⁰ Id. at *1-11.

²⁵⁷¹ 991 F.2d 511, 518-19 (9th Cir. 1993).

²⁵⁷² MDY Industries, 2008 U.S. Dist. LEXIS at *10-11.

licensed to exercise other rights of the copyright holder, such as distributing or modifying the software, thus establishing that the provisions of the license were designed to protect Blizzard's copyright interests. Thus, when end users used bot software such as Glider to operate the WoW game client software in violation of the EULA and TOU, they were making unauthorized copies of the game client software, which infringed Blizzard's copyright, and for which the defendant was liable as a copyright infringer.²⁵⁷³

The district court rejected the defendant's argument that the copies of the game client software made by end users while operating the Glider software were authorized by Section 117 of the copyright statute. The court noted that MAI and at least two other rulings by the Ninth Circuit had held that licensees of a computer program do not "own" their copy and are therefore not entitled to a Section 117 defense.²⁵⁷⁴ In October of 2008, the court awarded Blizzard over \$6 million in damages for copyright infringement.²⁵⁷⁵

On appeal, the Ninth Circuit confirmed the district court's ruling that WoW players were licensees, not owners, of their copy of WoW's game client software. Citing the standards for determining status as a licensee versus an owner in its decision in Vernor v. Autodesk,²⁵⁷⁶ the Ninth Circuit noted that Blizzard reserved title in the software, granted players a non-exclusive, limited license, and also imposed transfer restrictions if a player sought to transfer the license and a variety of use restrictions (e.g., for non-commercial entertainment purposes only and no use in cyber cafes and computer gaming centers). Accordingly, WoW players were licensees, not owners, of their copy of the software and therefore did not have rights under Section 117.²⁵⁷⁷

The Ninth Circuit then turned to whether the prohibition on the use of bots and cheats was a contractual covenant or a condition on the license. Section 4(B) of the TOU provided:

You agree that you will not ... (ii) create or use cheats, bots, "mods," and/or hacks, or any other third-party software designed to modify the World of Warcraft experience; or (iii) use any third-part software that intercepts, "mines," or otherwise collects information from or through the Program or Service.²⁵⁷⁸

The court noted that, wherever possible, equity construes ambiguous contract provisions as covenants rather than conditions. The court found that TOU sections 4(B)(ii) and (iii)'s prohibitions against bots and unauthorized third-party software were covenants rather than

²⁵⁷³ Id. at *12-18.

²⁵⁷⁴ Id. at *24-28.

²⁵⁷⁵ Liz McKenzie, "Warcraft Creator Wins \$6M Over Software 'Bot,'" *Law360* (Oct. 1, 2008), available as of Oct. 2, 2008 at <http://ip.law360.com/articles/71118>.

²⁵⁷⁶ 621 F.3d 1102, 1108-09 (9th Cir. 2010).

²⁵⁷⁷ MDY Industries, LLC v. Blizzard Entertainment, Inc., 2011 U.S. App. LEXIS 3428 at *12-14 (9th Cir. Feb. 17, 2011).

²⁵⁷⁸ Id. at *11.

copyright-enforceable conditions. Nothing in those provisions conditioned Blizzard's grant of a limited license on players' compliance with the restrictions in TOU Section 4(B).²⁵⁷⁹

The court further noted that, although one can be liable for copyright infringement by exceeding the scope of a granted license, the potential for infringement exists only where the licensee's action exceeds the license's scope in a manner that implicates one of the licensor's exclusive statutory copyright rights, such as unlawful reproduction or distribution. Although a Glider user violated the anti-bot covenants with Blizzard, the user did not thereby commit copyright infringement because Glider did not infringe any of Blizzard's exclusive rights. For instance, the use did not alter or copy WoW software.²⁵⁸⁰

Were we to hold otherwise, Blizzard – or any software copyright holder – could designate any disfavored conduct during software use as copyright infringement, by purporting to condition the license on the player's abstention from the disfavored conduct. The rationale would be that because the conduct occurs while the player's computer is copying the software code into RAM in order for it to run, the violation is copyright infringement. This would allow software copyright owners far greater rights than Congress has generally conferred on copyright owners.²⁵⁸¹

Accordingly, the Ninth Circuit held “that for a licensee's violation of a contract to constitute copyright infringement, there must be a nexus between the condition and the licensor's exclusive rights of copyright.”²⁵⁸² Here, the WoW players did not commit copyright infringement by using Glider in violation of the TOU. MDY was thus not liable for secondary copyright infringement, because there was no direct infringement on the part of the players.²⁵⁸³

(j) **Louis Vuitton v. Akanoc Solutions, Inc.**

In Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.,²⁵⁸⁴ the defendants provided OSP services that hosted websites through which the plaintiff alleged goods were being sold that infringed its trademarks and copyrights. The plaintiff sought to hold the defendants contributorily and vicariously liable for hosting such websites and the defendants moved for summary judgment. The court denied the motion as to contributory infringement, but granted it

²⁵⁷⁹ Id. at *16-17.

²⁵⁸⁰ Id. at *18.

²⁵⁸¹ Id. at *20.

²⁵⁸² Id. at *21. The court noted, however, special treatment in the case of failure to pay: “A licensee arguably may commit copyright infringement by continuing to use the licensed work while failing to make required payments, even though a failure to make payments otherwise lacks a nexus to the licensor's exclusive statutory rights. We view payment as *sui generis*, however, because of the distinct nexus between payment and all commercial copyright licenses, not just those concerning software.” Id. at *22 n.4.

²⁵⁸³ Id. at *21-22.

²⁵⁸⁴ 591 F. Supp. 2d 1098 (N.D. Cal. 2008), aff'd in part & rev'd in part, 658 F.3d 936 (9th Cir. 2011).

as to vicarious infringement.²⁵⁸⁵ With respect to contributory infringement, the court found issues of material fact concerning whether direct infringements were taking place on websites hosted by the defendants, citing internal emails in which defendants discussed attempts to take down websites selling counterfeit Louis Vuitton products.²⁵⁸⁶ The court also found issues of material fact with respect to the defendants' knowledge of infringing activity, rejecting the defendants' argument that they did not have such knowledge because they did not log on to sites to investigate complaints of infringing activity, but rather simply took such sites down. The court found this testimony merely served to highlight that there were issues of material fact concerning actual knowledge on the part of defendants, and in any event, the defendants had not submitted any testimony with respect to whether they should have known of infringing activity in view of numerous letters from the plaintiff alleging such activity.²⁵⁸⁷

Finally, citing the Ninth Circuit's decision in Perfect 10 v. Amazon allowing a finding of material contribution where an OSP fails to take "simple measures" to limit infringement on its site, the court found material issues of fact with respect to whether the defendants could have taken such simple measures based on evidence submitted by the plaintiff that the defendants had the ability to remove single websites by disabling IP addresses without taking down an entire server. The court noted that the defendants had not submitted any evidence indicating that removing a web site in this fashion would not be a "simple measure" by which they could purge infringing activity using their services.²⁵⁸⁸

A jury found the defendants liable for willful contributory infringement and awarded statutory damages, and found that the defendants were not entitled to the safe harbors of the DMCA. After the verdict, the defendants filed a motion for JMOL with respect to the claims and the DMCA defense.²⁵⁸⁹ The court denied the defendants' motion as to the contributory copyright claim. With respect to the knowledge requirement, the evidence established that the defendants had ample actual notice of directly infringing activity on dozens of web sites hosted on the defendants' servers in the form of many notice letters from the plaintiff identifying specific web sites that were selling counterfeit goods infringing the plaintiff's copyrights.²⁵⁹⁰ With respect to the material contribution requirement, the defendants provided and operated the servers through which the web sites offering the counterfeit goods were hosted, and continued to do so despite receiving notices from the plaintiff of particular web sites engaged in infringing conduct. One of the defendants testified that he rarely used several of the tools at his

²⁵⁸⁵ Id. at 1113. The court's rulings with respect to vicarious infringement are set forth in Section III.C.3(i) below.

²⁵⁸⁶ Id. at 1106.

²⁵⁸⁷ Id. at 1107-08.

²⁵⁸⁸ Id. at 1108-09.

²⁵⁸⁹ Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., 2010 U.S. Dist. LEXIS 85266 at *1-2 (N.D. Cal. Mar. 19, 2010), aff'd in part & rev'd in part, 658 F.3d 936 (9th Cir. 2011).

²⁵⁹⁰ Id. at *17.

disposal to punish or deter the operation of the counterfeiting web sites. Thus, there was sufficient evidence to support a finding by the jury of material contribution.²⁵⁹¹

Accordingly, the court issued a permanent injunction against ‘knowingly’ hosting infringing web sites in the United States. The order specifically spelled out that the defendants would be deemed to be acting “knowingly” upon proof that (i) they had been served by email or regular mail by the plaintiff with a notice of infringement of specific copyrights on an Internet hosting or routing service operated by the defendants, and (ii) the notice contained screen shot(s) depicting the infringing activity, and (iii) 72 hours after service of the notice the infringing activity was still taking place. The order further stated that the defendants would not be deemed to be acting “knowingly” upon proof that (i) the defendants condition their use of their Internet hosting or routing services, and notify each subscriber and customer accordingly, that their use of such services is subject to immediate termination upon receipt of a notice of infringement that the subscriber or customer is infringing the copyright of Louis Vuitton, and (ii) the defendants publish on their web site complete and accurate contact information for receiving notices of infringement, and (iii) upon receipt of a notice the defendants mailed to the plaintiff an acknowledgment of receipt, and (iv) the defendants assigned a tracking number to the notice, and (v) within 24 hours of receipt of the notice the defendants sent to the subscriber or customer a notice to immediately cease and desist from the activity that is the subject of the notice and failure to do so would result in immediate termination of services, and (vi) the defendants investigated whether activity did or did not cease within the time period required by the notice and upon verifying that it did not cease, the defendants immediately terminated services to the infringing subscriber or customer.²⁵⁹²

On appeal, the defendants challenged the jury instructions on contributory infringement as erroneous because they “omitted both the elements of intent and material contribution.”²⁵⁹³ Although the court agreed with the defendants that the jury instructions departed from the Ninth Circuit Model Jury Instructions, the Ninth Circuit rejected the defendants’ challenge, noting that the court had never held that an express finding of intent is necessary to support liability for contributory infringement. Thus, the district court was not required to instruct the jury to make a separate finding that the defendants’ knowing action evidenced intent to contribute to copyright infringement. In addition, the court rejected the defendants’ argument that the jury instructions should have required an express finding of material contribution. The court noted that material contribution turns on whether the activity in question substantially assists direct infringement, and here, there was no question that providing direct infringers with server space satisfied that standard. Thus, the district court had not erred by narrowing the

²⁵⁹¹ Id. at *20.

²⁵⁹² Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., 2010 U.S. Dist. LEXIS 34021 at *4-6 (N.D. Cal. Mar. 19, 2010).

²⁵⁹³ Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc., 658 F.3d 936, 943 (9th Cir. 2011).

instruction on material contribution to the only genuine question as to that element – whether the defendants provided their services to direct infringers.²⁵⁹⁴

The court also rejected the defendants’ challenge to the court’s instructions on willful infringement, on the ground that the instructions erroneously allowed the jury to find that the defendants engaged in willful infringement based solely on a finding of knowing contribution to direct infringement. The defendants claimed that under this formulation, a finding of willfulness required proof of no element beyond those of contributory copyright infringement. The court rejected this argument, noting that a finding of willfulness in the copyright context can be based on either intentional behavior or merely reckless behavior or willful blindness to the copyright holder’s rights. The jury instructions were adequate under this standard.²⁵⁹⁵

Finally, the court determined that the jury’s award of statutory damages was erroneous. The jury awarded statutory damages of \$300,000 per defendant for willful contributory infringement of two of Louis Vuitton’s copyrights. The court held that the jury verdict form erroneously invited the jury to specify a separate statutory damages award against *each* defendant.²⁵⁹⁶ “Statutory damages reach a maximum based on the number of protected works, not the number of defendants.”²⁵⁹⁷ Accordingly, the court reversed the statutory damages award and remanded with instructions that the district court award statutory damages in the total amount of \$300,000, for which the defendants would be jointly and severally liable.²⁵⁹⁸

(k) Arista Records v. Usenet.com

In Arista Records LLC. v. Usenet.com, Inc.,²⁵⁹⁹ the defendants operated a Napster-like Usenet service that advertised to and targeted users who wanted to download music files. Unlike peer-to-peer filing sharing networks, the files were stored on “spool” news servers operated by the defendants.²⁶⁰⁰ The court granted the plaintiff record companies’ motion for summary judgment on their claim for contributory infringement. With respect to the knowledge prong of contributory liability, unlike the Ninth Circuit in the Napster cases, the court ruled that knowledge of specific infringements on the defendants’ service was not required to support a finding of contributory infringement. Rather, it was sufficient that the record established the defendants’ employees were clearly aware that their service was used primarily to obtain copyrighted material, users of the service told defendants’ technical support employees that

²⁵⁹⁴ Id. at 943-44.

²⁵⁹⁵ Id. at 944.

²⁵⁹⁶ Id. at 946.

²⁵⁹⁷ Id. at 947.

²⁵⁹⁸ Id.

²⁵⁹⁹ 633 F. Supp. 2d 124 (S.D.N.Y. 2009).

²⁶⁰⁰ Id. at 130-31.

they were engaged in copyrighted infringement, and the defendants had targeted the service to former users of Napster and Kazaa.²⁶⁰¹

The material contribution prong was satisfied because the defendants' servers were the sole instrumentality of their subscribers' infringement. The servers physically stored the content that subscribers requested for download, and the defendants had created designated servers for newsgroups containing MP3 or music binary files so as to maximize the average retention time of those files as compared to other Usenet groups with non-music content. The court rejected the defendants' assertion that they could not be contributorily liable under the Supreme Court's Sony doctrine because their product had substantial noninfringing uses. The court distinguished Sony on the ground that Sony's last meaningful contact with the product or the purchaser was at the point of purchase, after which it had no ongoing relationship with the product or its end user. By contrast, the defendants maintained an ongoing relationship with their infringing users in the course of offering their service, thereby rendering the noninfringing uses immaterial to insulate the defendants from liability. Accordingly, the court granted the plaintiffs' motion for summary judgment on their contributory copyright infringement claim.²⁶⁰²

(I) Hermeris v. Brandenburg

In Hermeris v. Brandenburg,²⁶⁰³ the court issued a ruling that may impliedly broaden an online service provider's duty to police its site for other similar infringing material, at least in a situation where no DMCA safe harbor has been asserted and the material is all owned by related defendants. The plaintiff operated an online document preparation web site. The plaintiff sought to hold the defendant OSP contributorily and vicariously liable for hosting three web sites, all of which were owned by apparently related defendants, that were allegedly infringing of the plaintiff's copyrights in its own web site. The plaintiff gave the OSP direct notice that the first of the three web sites was infringing, then sought to hold the OSP secondarily liable for failure to take down the second and third web sites, which the plaintiff alleged were substantially similar to the first web site. The OSP filed a motion to dismiss.²⁶⁰⁴

The court denied the motion with respect to contributory liability because, assuming the facts pled in the complaint were true, the OSP had constructive knowledge of infringement by virtue of the fact that it had received actual knowledge of infringement by the first web site and the fact that the second and third web sites were substantially similar to the first web site.²⁶⁰⁵ "Given these factual allegations and viewing the facts in the light most favorable to plaintiff, it is reasonable to infer that [the OSP] should have known that the Second and Third Websites

²⁶⁰¹ Id. at 154-55.

²⁶⁰² Id. at 155-56.

²⁶⁰³ 2011 U.S. Dist. LEXIS 6682 (D. Kan. Jan. 23, 2011).

²⁶⁰⁴ Id. at *4-6.

²⁶⁰⁵ Id. at *10.

directly infringed upon plaintiff's copyright."²⁶⁰⁶ Although the court does not say, its ruling that the actual notice of infringement by the first web site gave the OSP constructive knowledge of infringement by the second and third web sites may have been influenced by the fact that all three web sites were owned by the same defendants and were all substantially similar to each other. If so, then the court's ruling may not necessarily imply a more general holding that actual notice of one infringement gives a defendant OSP constructive notice as to all other substantially similar material on its site for purposes of contributory liability. In any event, having found sufficient knowledge for purposes of contributory liability, the court found an adequate allegation of material contribution to infringement in the form of failure to purge the web sites from the OSP's system.²⁶⁰⁷

The court also ruled that the plaintiff had adequately pled a claim for vicarious infringement because it had pled that the OSP hosted the infringing web sites, and the court found it reasonable to assume that, as the host, the OSP had the right and ability to stop or limited the defendants from displaying or distributing the allegedly infringing materials. The court rejected the OSP's argument that it did not have control over the second and third web sites because it did not have actual knowledge of them. The court found it sufficient for purposes of the control prong that the plaintiff had pled the OSP had constructive knowledge of the second and third web sites.²⁶⁰⁸ This ruling seems to imply that, at least in an Internet context (as opposed to a dance hall, for example), some form of knowledge of infringing activity is required before a defendant can be said to have control over it.

The court's opinion makes no mention of the OSP asserting any safe harbor defense under Section 512.

(m) Flava Works v. Gunter

The facts of this case are set forth in Section III.C.1(b). The court denied the defendants' motion to dismiss the plaintiff's claim for contributory infringement. With respect to the knowledge requirement, the court assumed for its discussion that to allege knowledge for common law liability, a plaintiff must allege something more than the defendants' receipt of its seven DMCA notices. Here the DMCA notices identified both specific infringing files and specific repeat infringers. In addition, although the plaintiff did not allege that the defendants failed to remove the infringing material from myVidster, it did allege that the defendants failed to take any action to stop, reprimand, or ban the repeat infringers listed in the DMCA notices and that the defendants failed to implement filters or identifiers to prevent repeated infringing conduct.²⁶⁰⁹ "Because plaintiff alleges not just the receipt of DMCA notices but also that after having received the notices defendants failed to act to prevent future similar infringing conduct,

²⁶⁰⁶ Id.

²⁶⁰⁷ Id. at *11.

²⁶⁰⁸ Id. at *12-13.

²⁶⁰⁹ Flava Works, Inc. v. Gunter, 2011 U.S. Dist. LEXIS 50067 at *11-12 (N.D. Ill. May 10, 2011), rev'd, 689 F.3d 754 (7th Cir. 2012).

it has sufficiently alleged the knowledge element of contributory copyright infringement.”²⁶¹⁰ The court found a sufficient material contribution alleged in the allegations that defendants provided a web site that stored infringing material, allowed backup copies to be made, encouraged sharing, had no filters or identifiers in place to prevent repeat infringers, and took no action to stop or ban the repeat infringers who allegedly posted the plaintiff’s copyrighted works.²⁶¹¹

In a subsequent opinion, the court ruled that the plaintiff was entitled to a preliminary injunction, finding the defendant liable for contributory infringement for essentially the same reasons articulated in the first opinion.²⁶¹² In its opinion, the court commented on the provisions of a proposed injunction submitted by the plaintiff. The plaintiff had proposed that myVidster be required to implement digital fingerprinting on its site, but the court noted that the plaintiff had presented no evidence of what constituted “digital fingerprinting” or whether its implementation would be reasonably feasible or affordable. Accordingly, the court said it would decline to order that the defendants implement that technology. However, the court agreed that it would include in the injunction an obligation to filter based on a list of keywords and tags to prevent the upload or download of, posting of links to videos, and the posting of embedded videos containing the plaintiff’s copyrighted content, including intentional or inadvertent misspellings of the keywords and tags. The injunction would also require the defendants to disable the accounts of users who on two or more occasions had posted content that infringed one or more of the plaintiff’s copyrights.²⁶¹³

On appeal, the Seventh Circuit (per Judge Posner) vacated the preliminary injunction in a rather confusing opinion. The court first adopted the Second Circuit’s succinct definition of contributory infringement as “personal conduct that encourages or assists the infringement.”²⁶¹⁴ The court then considered two potential infringing acts of myVidster users to which myVidster might be a contributory infringer – the uploading of infringing copies of Flava’s videos and the public performance of those videos when viewed by myVidster users. The court held that myVidster could not be a contributory infringer to any unauthorized acts of uploading of infringing copies of Flava’s videos because there was no evidence that myVidster was encouraging such acts, and merely providing a connection to websites that contained illegal copies of Flava’s copyrighted videos was insufficient encouragement for contributory liability.²⁶¹⁵ “myVidster displays names and addresses (that’s what the thumbnails are, in effect) of videos

²⁶¹⁰ Id. at *12.

²⁶¹¹ Id. at *12-13.

²⁶¹² Flava Works, Inc. v. Gunter, 2011 U.S. Dist. LEXIS 82955 at *20-29 (N.D. Ill. July 27, 2011), rev’d, 689 F.3d 754 (7th Cir. 2012). The court also ruled that the defendants were not entitled to a DMCA safe harbor. See Section III.C.6(b)(1)(iii).r below.

²⁶¹³ Id. at *34-35.

²⁶¹⁴ Flava Works, Inc. v. Gunter, 689 F.3d 754, 757 (7th Cir. 2012) (quoting Matthew Bender & Co. v. West Publishing Co., 158 F.3d 693, 706 (2d Cir. 1998)).

²⁶¹⁵ Flava Works, 689 F.3d at 757-58.

hosted elsewhere on the Internet that may or may not be copyrighted. Someone who uses one of those addresses to bypass Flava's pay wall and watch a copyrighted video for free is no more a copyright infringer than if he had snuck into a movie theater and watched a copyrighted movie without buying a ticket. The facilitator of conduct that doesn't infringe copyright is not a contributory infringer."²⁶¹⁶

The court then turned to whether myVidster could be a contributory infringer to unauthorized public performances of Flava's videos. With no direct analysis of the statutory definition of "public performance," Judge Posner posited two different interpretations of what constitutes a public performance under the transmit clause of the definition. The first interpretation, which he labeled "performance by uploading," is that "uploading plus bookmarking a video is a public performance because it enables a visitor to the website to receive (watch) the performance at will, and the fact that he will be watching it at a different time or in a different place from the other viewers does not affect its 'publicness,' as the statute makes clear."²⁶¹⁷ myVidster could have no contributory liability under this interpretation because there was no evidence that myVidster was contributing to the decision of users to upload a Flava video to the Internet where it then became available to be bookmarked on myVidster's web site.²⁶¹⁸

The second interpretation, which Judge Posner labeled "performance by receiving," is that "the performance occurs only when the work (Flava's video) is transmitted to the viewer's computer – in other words when it is 'communicated to the public in a form in which the public can visually or aurally comprehend the work.'"²⁶¹⁹ The court noted that under this interpretation, there was an argument that even though the video uploader was responsible for the transmitting, not myVidster, myVidster was assisting the transmission by providing the link between the uploader and the viewer, and was thus facilitating public performance. However, Judge Posner ultimately rejected such an argument by virtue of distinctions from previous Seventh Circuit authority in the Fonovisa and Aimster cases.

Specifically, Judge Posner distinguished the present case from the "swap meet" operated by the defendant in the Fonovisa case,²⁶²⁰ in which pirated copies of musical recordings were being bought and sold. The court noted that Flava's pirated videos were not sold, and there wasn't even admissible evidence that they were actually being accessed via myVidster, rather than via other websites. myVidster was not encouraging the uploading of Flava videos because it had some financial incentive to encourage performance of those works, as the swap meet

²⁶¹⁶ Id. at 758.

²⁶¹⁷ Id. at 760.

²⁶¹⁸ Id. at 761.

²⁶¹⁹ Id. at 760 (quoting William F. Patry, Patry on Copyright § 14:21, p. 14-41 (2012)).

²⁶²⁰ Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996).

did.²⁶²¹ Judge Posner also distinguished the Aimster case,²⁶²² in which Aimster created the online equivalent of a swap meet by supplying the software that enabled the file-sharing of copyrighted recordings over the Internet. Unlike Aimster, myVidster was not encouraging swapping, which in turn would encourage infringement.²⁶²³

Accordingly, the court concluded that on the record compiled to that point there was no basis for the grant of a preliminary injunction on the grounds of secondary infringement. Judge Posner noted, however, that Flava should be entitled to an injunction against myVidster's backup service, in which it made copies of videos that some of its subscribers had posted, including videos copyrighted by Flava (although myVidster had stopped offering that service), because the service constituted direct infringement on myVidster's part. But the preliminary injunction issued by the district court did not enjoin the backup service because Flava didn't make a claim for direct infringement a basis for its motion for preliminary relief. Judge Posner noted that such an injunction might be something for consideration on remand.²⁶²⁴

(n) Perfect 10 v. Giganews

The District Court Proceedings

In Perfect 10, Inc. v. Giganews, Inc.²⁶²⁵ the defendants (Giganews and Livewire) were providers of access to USENET for a monthly fee starting at \$4.99 per month. The content posted by the defendants' subscribers and other USENET users, including infringing content, was stored on the defendants' servers. Before filing its complaint, the plaintiff sent a letter to one of the defendants, Giganews, notifying that it was infringing the plaintiff's copyrights, and included a DVD containing hundreds of Perfect 10 images, characterizing them as a sampling of its copyrighted materials that Giganews' site had offered for sale without authorization. Giganews responded by stating that each article posted on USENET has a unique message identification number, and if the plaintiff provided the identification numbers of the articles containing the infringing content, Giganews would be able to find the specific infringing material and remove it. The plaintiff did not do so. The plaintiff then filed a complaint for direct, contributory and vicarious copyright infringement and the defendants moved to dismiss all claims.²⁶²⁶

Concerning the claims of copyright infringement, the court noted that the plaintiff's complaint was unclear as to the facts supporting those claims, but it appeared to be basing them on the following allegations: "(1) that Defendants are USENET providers who charge their subscribers a fee; (2) that Defendants program their computers to copy USENET content from

²⁶²¹ Flava Works, 689 F.3d at 761-62.

²⁶²² In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004).

²⁶²³ Flava Works, 689 F.3d at 762.

²⁶²⁴ Id. at 762-63.

²⁶²⁵ 2013 U.S. Dist. LEXIS 71349 (C.D. Cal. Mar. 8, 2013).

²⁶²⁶ Id. at *1-7.

other USENET servers and make this content available to their subscribers; (3) that USENET is now primarily used by its subscribers or visitors to exchange pirated content; (4) that Defendants are not only aware of the rampant piracy committed by USENET users but rely on the piracy as part of their business model; and (5) that Plaintiff has found at least 165,000 unauthorized Perfect 10 images on Defendants' USENET service."²⁶²⁷

With respect to the plaintiff's claim of contributory liability, the court first considered the knowledge requirement. The defendants, citing the Ninth Circuit's decision in Napster that the knowledge requirement is satisfied when a computer system operator learns of specific infringing material available on the system and fails to purge it, argued that because knowledge must be of "specific" material, a defendant must know the copyright registration number and the specific location of the infringing content in order to be liable. The court rejected this, holding that it is enough if the defendant has sufficient information to be able to find the specific infringing content on its system. In this case, the plaintiff's allegations that it sent Giganews a notice that identified hundreds of Perfect 10 copyrighted images that it had found using the defendants' service, some of which displayed a copyright notice, and that Giganews had a search function which it could have used to search for the infringing content based on the image identifiers the plaintiff provided in its notice, were sufficient to support the plaintiff's claim that Giganews had knowledge of the content infringing the plaintiff's copyrights. Discovery might yield facts that could lead a jury to conclude that it would have been easy for Giganews to find specific infringing content, or might reveal that the information provided by the plaintiff was not enough to identify any infringing articles. But the plaintiff had pled enough facts to give rise to a plausible inference that Giganews knew of specific infringing Perfect 10 images on its servers.²⁶²⁸

On the other hand, the complaint did not adequately plead that defendant Livewire knew of specific infringing works. The plaintiff had not alleged that it or anyone else notified Livewire of unauthorized Perfect 10 images on its servers. Thus, the plaintiff was forced to rely only on its allegation that Livewire knew generally that USENET was used to exchange pirated content. That was precisely the type of general knowledge rejected by the Supreme Court in Sony, and the plaintiff had therefore failed to adequately plead a claim for contributory infringement against Livewire.²⁶²⁹

With respect to the material contribution requirement, the court ruled the plaintiff's allegations that the defendants provided access to USENET, a system that was widely known to be a source of pirated content, and that the defendants' storage of USENET content on their servers facilitated the exchange of pirated works among the defendants' subscribers and other USENET users, were sufficient to allege that the defendants materially contributed to the infringement. Accordingly, the court denied the defendants' motion to dismiss the contributory

²⁶²⁷ Id. at *12-13.

²⁶²⁸ Id. at *29-32.

²⁶²⁹ Id. at *32.

infringement claim with respect to Giganews, but dismissed the contributory infringement claim against Livewire with leave to amend.²⁶³⁰

Turning to the claims of vicarious liability, the court denied the defendants' motion to dismiss those claims. With respect to the direct financial benefit prong, the court held that the plaintiff's allegations that interest in USENET is now largely centered around alt.binaries* newsgroups and that the defendants' ability to generate monthly subscriptions and revenues was based almost exclusively on the demand for pirated copyrighted works contained in the alt.binaries* hierarchies were sufficient to establish that the defendants enjoyed a direct financial benefit from the infringing content on their servers.²⁶³¹ The court rejected the defendants' invitation to interpret the Netcom and Ellison cases as establishing a categorical rule that fixed fees preclude a finding of a direct financial benefit as a matter of law. Rather, those cases found no causal relationship between the fixed fee charged by the defendants and the infringing activity of their subscribers.²⁶³²

With respect to the control element of vicarious liability, the court found sufficient control on the part of Giganews from the fact that its Terms of Use clearly stated that it had the power to suspend and cancel the accounts of its users, and the fact that the plaintiff had alleged that Giganews could easily find unauthorized Perfect 10 images on its servers by using its search function. The plaintiff had not, however, alleged any facts showing what control Giganews exerted over USENET users who were not Giganews subscribers. Nor had the plaintiff alleged any facts that Livewire had any power over third party infringers. Accordingly, the court ruled that the plaintiff had stated a claim for vicarious liability against Giganews for copyright infringement by Giganews subscribers only, but the vicarious liability claim against Livewire must be dismissed with leave to amend.²⁶³³

The plaintiffs amended the complaint and the defendants again moved to dismiss. Giganews contended that the new allegations concerning the plaintiff's notices demonstrated that its secondary infringement claims failed. A different judge (Judge Collins) disagreed and found it unnecessary to revisit Judge Matz's conclusion that the secondary infringement allegations against Giganews were adequate. Accordingly, the court considered only whether the plaintiff had now adequately pled secondary infringement claims against Livewire.²⁶³⁴

With respect to the knowledge requirement of contributory infringement, the court noted that it had reviewed every one of the 42 notices referenced in the amended complaint. Consistent with Judge Matz's order, Judge Collins found that those notices were specific enough to overcome a motion to dismiss because they might be sufficient to allow their recipient to

²⁶³⁰ Id. at *33.

²⁶³¹ Id. at *34-35.

²⁶³² Id. at *34-36.

²⁶³³ Id. at *38-40.

²⁶³⁴ Perfect 10, Inc. v. Giganews, Inc., 2013 U.S. Dist. LEXIS 98997 at *10 (C.D. Cal. July 10, 2013).

locate the referenced images on its servers. However, those notices were sent only to Giganews. Because the notices were addressed only to Giganews and made no mention of Livewire, and because the identifiers associated with the images might well not have been the same for both Giganews and Livewire, the notices were effective to inform only Giganews that the infringing images were on its servers. The notices therefore could not be effective as to Livewire and were an insufficient basis upon which to plead that Livewire had knowledge of the infringing conduct. The plaintiff's pleadings that Livewire also generally knew that it offered images that infringed were insufficient to plead knowledge for purposes of contributory infringement. The court therefore concluded that the plaintiff's contributory infringement claim against Livewire failed.²⁶³⁵

With respect to the vicarious liability claim, Judge Collins noted that Judge Matz's order had found that charging subscribers a fee was sufficient to show direct financial benefit, the plaintiff had pled that Livewire charged fees for access to infringing materials it provided, and that was adequate to show that Livewire directly benefited from the infringing activity of its clients. The court determined, however, that the plaintiff had not pled facts adequate to establish control. The plaintiff's allegations that Livewire controlled what it purchased from Giganews and provided to clients, and that Livewire controlled Giganews because it was owned, operated and/or controlled by the same parties, were insufficient to show that Livewire exercised control over the infringing activity of its clients. Accordingly, the court concluded that the plaintiff's vicarious infringement claims against Livewire failed.²⁶³⁶ Because the plaintiff had already amended its complaint once, and had not shown how any further amendment could cure its pleading deficiencies, the court dismissed the secondary infringement claims against Livewire without leave to amend.²⁶³⁷

After discovery, Giganews moved for partial summary judgment with respect to secondary copyright liability. A third judge (Judge Birotte) granted Giganews' motion.²⁶³⁸ Turning first to the financial benefit prong of vicarious liability, the court noted that financial benefit exists where the availability of infringing material acts as a draw for customers, and (citing the Ninth Circuit's Ellison decision) the size of the draw relative to a defendant's overall business is immaterial. However, the plaintiff was still required to prove a direct causal link between the infringing activities *at issue in this case* and a direct financial benefit to Giganews. Thus, the court ruled that the direct financial benefit requirement demanded more than evidence that customers were drawn to Giganews to obtain access to infringing material in general. Perfect 10 was required to prove with competent evidence that at least some of Giganews' customers were drawn to Giganews' services, in part, to obtain access to infringing *Perfect 10* material. Despite extensive discovery (which was closed), the record lacked, and Perfect 10 was unable to identify, a single piece of evidence to that effect. And even if the scope

²⁶³⁵ Id. at *11-12.

²⁶³⁶ Id. at *13-15.

²⁶³⁷ Id. at *15-16.

²⁶³⁸ Perfect 10, Inc. v. Giganews, Inc., U.S. Dist. LEXIS 183590 (C.D. Cal. Nov. 14, 2014).

of causation were expanded to the broader category of erotic images, there was no evidence that any customer was ever drawn to Giganews' services to obtain access to erotic images. Perfect 10's evidence that staggering amounts of copyrighted works owned by movie producers and television networks were available on Giganews' servers only emphasized that there was no evidence Giganews subscribers purchased Giganews' services in part because of the relatively miniscule number of Perfect 10 images available on the servers. If the universe of infringing material on USENET were as broad and diverse as Perfect 10 suggested, any conclusion that subscribers were drawn to Giganews' services as a result of the availability of Perfect 10 content would be impermissible pure speculation.²⁶³⁹

Nor was it sufficient that a Giganews customer may have posted or accessed copyrighted Perfect 10 material as an added benefit to a subscription. To survive summary judgment on vicarious infringement, the court ruled that Perfect 10 must produce significant probative evidence that at least some of Giganews' customers subscribed to the Giganews services at least partially for the purpose of accessing or posting Perfect 10's copyrighted material, or at least copyrighted erotic images. Perfect 10 had failed to do so. The court also rejected Perfect 10's contention that Judge Matz and Judge Collins had already ruled that the monthly fee charged by Giganews to its users to access allegedly infringing material constituted a direct financial benefit. Judge Birotte noted that, in his order on the defendants' first motion to dismiss, Judge Matz emphasized the importance of the procedural posture of the case in holding that Perfect 10 had adequately alleged a claim for vicarious infringement. Judge Matz had correctly observed that the operative question was whether there was a causal relationship between Perfect 10's infringing content and Giganews' subscription revenues. Judge Collins adopted Judge Matz's analysis and found that the same allegations were sufficient to advance the action past the pleadings stage. However, Judge Birotte concluded that, after full discovery, the evidence did not bear out Perfect 10's allegations that the availability of its copyrighted content was a draw for Giganews' customers, and Giganews was therefore entitled to summary judgment on the plaintiff's vicarious infringement claim.²⁶⁴⁰

Turning next to the claim for contributory infringement, Judge Birotte noted that one contributorily infringes when he has knowledge of another's infringement, and *either* materially contributes to or induces that infringement. Giganews contended that the inducement theory of contributory liability is the *only* theory of contributory liability after the Supreme Court's Grokster decision. Judge Birotte rejected this contention, citing Ninth Circuit cases that had repeatedly held that the two tests are alternative.²⁶⁴¹ Under either theory, however, the contribution to infringement must be intentional for liability to arise. Mere knowledge of

²⁶³⁹ Id. at *8-11.

²⁶⁴⁰ Id. at pp. 12-16.

²⁶⁴¹ Id. at *17-18. "Indeed, the 'material contribution' theory of contributory liability appears to be consistent with the Supreme Court's formulation that one may be liable for contributory infringement by *either* 'inducing or encouraging direct infringement.' Grokster, 545 U.S. at 930 (emphasis added). The Ninth Circuit's 'material contribution' theory of liability appears to be a restatement of the 'encouraging' theory of liability articulated by the Supreme Court in Grokster." Id. at *18 n.3.

infringing potential or of actual infringing uses does not subject a product distributor or service provider to liability. However, the element of intent may be imputed to include the natural and probable consequences of one's conduct. In the case of inducement to infringe, intent is manifested where the service provider has actual knowledge that specific infringing material is available using its system and fails to take reasonable and feasible steps to refrain from providing access to infringing images.²⁶⁴²

Under either form of contributory liability, Perfect 10 was required to prove that Giganews had actual knowledge of specific acts of infringement. With the exception of items brought to Giganews' attention through Perfect 10's DMCA takedown notices, the court found there was no evidence that Giganews ever had actual knowledge of any specific Perfect 10 images on its servers. The court rejected Perfect 10's contention that Giganews had constructive knowledge that every post submitted under the same email address used in an identified infringing message or using the same image identifier was infringing. The court noted that the basic structure of USENET posting makes it impossible to tell if two messages with the same sender email address are actually from the same person or whether two posts with the same image identifier actually contain the same image. The only information truly unique to a USENET post is its Message-ID.²⁶⁴³

With respect to the DMCA notices sent by Perfect 10 – which if they conformed to the requirements of Section 512(c) of the DMCA would confer actual knowledge on the part of Giganews – Judge Birotte noted that Judge Collins had already observed that Perfect 10's practice of sending Giganews screenshots of a newsreader window along with instructions to conduct searches of specific names within certain newsgroups, and instructing Giganews that all of the messages yielded by those searches on a certain date contained infringing material, failed to substantially comply with the requirements for a DMCA takedown notice. Even putting aside the fact that USENET material is constantly in a state of flux, Perfect 10's voluminous search-screenshot takedown notices would require a manual, line-by-line comparison of countless individual search results for each notice. And even Perfect 10's evidence revealed that its own search-criteria method yielded some messages that were non-infringing. Instead, the only undisputed method for consistently identifying a specific USENET message that Giganews could promptly remove was the post's Message-ID. Where Perfect 10's takedown notices included the relevant Message-ID, the evidence showed that Giganews promptly disabled access to the offending message.²⁶⁴⁴

Perfect 10 attempted to create a fact issue by pointing to 542 messages where Message-IDs were supplied and Giganews did not take the posts down. However, Perfect 10 had submitted those Message-IDs by faxing screen printouts with the Message-ID in small text, with the result that the Message-IDs were illegible, and Perfect 10 refused Giganews' request to resubmit the Message-IDs in legible format. The court found even more puzzling the fact that

²⁶⁴² *Id.* at *18-19.

²⁶⁴³ *Id.* at *19-23.

²⁶⁴⁴ *Id.* at *24-29.

Perfect 10 admitted it was aware of and had used software that allowed it to extract thousands of Message-IDs for messages it believed to be infringing in about ten seconds. There was evidence that using such software would require less than 15 minutes to extract Message-IDs for more than 90% of the infringing Perfect 10 content that Perfect 10 was aware of on Giganews' servers. But Perfect 10 did not take that simple step to protect its copyrights. The court therefore concluded that there was no evidence that Giganews had any knowledge, actual or constructive, of any specific infringing content other than those messages for which Perfect 10 provided legible Message-IDs. As to those messages, the evidence was undisputed that Giganews promptly blocked access to the infringing messages. Accordingly, the court ruled that Giganews was entitled to summary judgment in its favor on Perfect 10's contributory infringement claim.²⁶⁴⁵

Finally, the court noted that, by this order and its order with respect to direct liability (see the discussion in Section II.A.4(v) above), each of the three theories of copyright liability Perfect 10 alleged against Giganews and Livewire had been adjudicated in the defendants' favor (either by summary judgment or a motion to dismiss). Accordingly, the court entered final judgment in favor of Giganews and Livewire as to all claims by Perfect 10 in the case.²⁶⁴⁶

Perfect 10 then filed a motion for reconsideration of the court's order granting summary judgment in favor of Giganews on contributory infringement. The court rejected a scattershot of bases for reconsideration asserted by Perfect 10, finding none of them to have merit.²⁶⁴⁷ One point in the court's opinion is of particular interest. Perfect 10 argued that the court erred in finding the evidence undisputed that Giganews promptly blocked access to infringing messages as soon as it received actual or constructive notice in the form of legible Message IDs. On reconsideration, Perfect 10 identified 10 takedown notices it sent to Giganews using its search-and-screenshot method via email. Each of the screenshots displayed a Message ID for the randomly selected search result buried in the message header in the bottom right corner of the screen. For those 10 select searches, Perfect 10 noted a similar search more than a year later revealed the message was still available.²⁶⁴⁸

The court observed that, although these notices that were otherwise deficient under the DMCA's notice requirements may have legibly identified a single Message ID, Perfect 10's own evidence made clear that Giganews utilized an *automated* system for processing takedown notices. That automated system was essential to expeditiously processing takedown notices in view of the staggering volume of requests Giganews received. The court noted that Perfect 10 was well aware of this fact, but the evidence was undisputed that Perfect 10 obstinately refused to provide Message IDs in any form that would permit Giganews to process the requests through its automated system. Even after Perfect 10 identified a method of automatically extracting

²⁶⁴⁵ Id. at *29-32.

²⁶⁴⁶ Perfect 10, Inc. v. Giganews, Inc., 2014 U.S. Dist. LEXIS 183595 (C.D. Cal. Nov. 14, 2014).

²⁶⁴⁷ Perfect 10, Inc. v. Giganews, Inc., 2015 U.S. Dist. LEXIS 53733 (C.D. Cal. Mar. 6, 2015).

²⁶⁴⁸ Id. at *23-25.

Message IDs that it admitted would allow it to takedown more than 90% of the alleged infringing material on Giganews' servers in less than 48 hours using Giganews' automated systems, Perfect 10 refused to present its takedown notices in a form that would permit Giganews to find and address the allegedly infringing material expeditiously.²⁶⁴⁹

The court further noted that, even in their legible emailed form, the evidence was undisputed that Perfect 10's insistence on its search-and-screenshot method presented only the Message IDs (to the extent it provided them at all) as non-searchable, secondary information in a larger image file, making it impossible for Giganews to use that information in its automated systems.²⁶⁵⁰ "As Perfect 10 acknowledges, its notices identified *search terms* rather than *specific content*. This is fatal under the DMCA, which requires a compliant notice identify *both* the specific infringing content *and* an effective means of locating that content."²⁶⁵¹ Perfect 10 had the ability to simply copy and paste the Message ID from its newsreader software and compile it in a file that Giganews could have quickly and efficiently processed through its automated DMCA takedown process. While a valid DMCA notice including a legible Message ID would have given Giganews actual or constructive knowledge of specific infringement, the court found that the 10 DMCA notices Perfect 10 identified in its motion for reconsideration were not such notices.²⁶⁵² And Giganews had no obligation under the DMCA to redesign its entire takedown system to accommodate Perfect 10's screenshot method, even if other service providers had systems more amenable to them.²⁶⁵³ Accordingly, the court rejected Perfect 10's notice arguments as a basis for reconsideration.

The Ninth Circuit's Decision

On appeal, the Ninth Circuit affirmed the district court's rulings with respect to contributory, inducement and vicarious liability. The Ninth Circuit began by noting that inducement is a separate basis for liability, although it is a part of the umbrella of contributory liability: "[O]ne contributorily infringes when he (1) has knowledge of another's infringement and (2) either (a) materially contributes to or (b) induces that infringement."²⁶⁵⁴ The court declined to reach the issue of whether the district court erred in finding that Giganews lacked actual knowledge, because it concluded that Perfect 10 failed to establish that Giganews materially contributed to or induced infringement of Perfect 10's copyrights.²⁶⁵⁵

²⁶⁴⁹ Id. at *26-27.

²⁶⁵⁰ Id. at *27-28.

²⁶⁵¹ Id. at *28 (emphasis in original).

²⁶⁵² Id. at *29-30.

²⁶⁵³ Id. at *30 n.9.

²⁶⁵⁴ Perfect 10, Inc. v. Giganews, Inc., 847 F.3d 657, 670 (9th Cir. 2017) (quoting Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 795 (9th Cir. 2007)).

²⁶⁵⁵ Id. at 670.

With respect to material contribution, the court noted that in the online context, a computer system operator is liable under a material contribution theory of infringement if it has actual knowledge that specific infringing material is available using its system and can take simple measures to prevent further damage to copyrighted works, yet continues to provide access to infringing works. Under the facts of the case at hand, the Ninth Circuit ruled that there were no simple measures available that Giganews failed to take to remove Perfect 10's works from its servers. Giganews presented sufficient evidence that Perfect 10's proposed method for locating infringing messages was onerous and unreasonably complicated. Giganews calculated that Perfect 10's method would require 354,000 hours of manual work for every 10 million Message-IDs, the number of Message-IDs that Giganews received every month. And Perfect 10 had not disputed that Giganews could easily remove infringing content if it was provided with automated Message-IDs. The court noted that Perfect 10's proffered evidence appeared to relate only to its argument that, by providing search results and search terms, Giganews could have searched for and found Message-IDs. But, as Giganews argued and the district court agreed, that method was unreliable and burdensome and therefore was not a reasonable and feasible means of preventing further damage to Perfect 10's copyrighted works. Accordingly, the Ninth Circuit concluded that Giganews was not able to take simple measures to remove infringing materials from its servers and therefore Perfect 10's first theory of contributory infringement liability failed.²⁶⁵⁶

With respect to inducement liability, the court noted that it requires four elements: (1) the distribution of a device or product, (2) acts of infringement, (3) an object of promoting its use to infringe copyright, and (4) causation. The court concluded that, based on the record, no reasonable juror could conclude Giganews distributed its product with the object of promoting its use to infringe copyright. Perfect 10 argued that Giganews had the object of promoting infringement because it offered 25,000 terabytes of copyrighted materials without permission, continued to commercially exploit the content of known repeat infringers, and advertised that it did not keep track of subscriber downloads, effectively encouraging infringement. The Ninth Circuit ruled that, even if true, none of that conduct suggested that Giganews clearly expressed an intent to promote infringement or took affirmative steps to foster infringement. The court therefore affirmed the district court's grant of summary judgment in favor of Giganews as to Perfect 10's contributory infringement claim.²⁶⁵⁷

With respect to vicarious liability, the court noted that it requires two elements on the part of the defendant: (1) the right and ability to supervise the infringing conduct and (2) a direct financial interest in the infringing activity. Financial benefit exists where the availability of infringing material acts as a draw for customers, and the size of the draw relative to a defendant's overall business is immaterial. The essential aspect of the direct financial benefit inquiry is whether there is a causal relationship between the infringing activity and any financial benefit a defendant reaps, regardless of how substantial the benefit is in proportion to a defendant's overall profits. Importantly, the Ninth Circuit ruled that the district court correctly

²⁶⁵⁶ *Id.* at 671-72.

²⁶⁵⁷ *Id.* at 672.

held that the financial benefit must be derived from the infringing activity in the case at hand,²⁶⁵⁸ meaning “infringement of the plaintiff’s copyrighted material, rather than general infringement.”²⁶⁵⁹ Thus, contrary to Perfect 10’s suggestion, the Ninth Circuit noted that a court is not required to hold a defendant vicariously liable regardless of whether there is any causal link between the infringement of the plaintiff’s own copyrighted works and any profit to the service provider.²⁶⁶⁰

Here, Perfect 10 argues for a rule that would allow a court to hold Giganews liable under a theory of vicarious liability by showing only that Giganews benefits financially from the infringement of *another’s* works, regardless of whether Giganews received any financial benefit from the specific infringement alleged. Such a rule would allow cases to be built on the rights of owners and the actions of users not before the court. At the very least, Perfect 10’s proposed rule is in significant tension with *Article III’s* standing requirement. At most, Perfect 10’s view runs counter to the requirement that there be a “causal connection between the injury and the conduct complained of[.]” Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).²⁶⁶¹

Accordingly, Perfect 10 was required to provide evidence that customers were drawn to Giganews’ services because of the infringing Perfect 10 material at issue. The court found there was no evidence indicating that anyone subscribed to Giganews because of infringing Perfect 10 material. Perfect 10 provided evidence suggesting only that some subscribers joined Giganews to access infringing material generally. The district court had therefore not erred in finding that Giganews did not receive a direct financial benefit from the infringement in this case, and the Ninth Circuit therefore did not need to address whether Giganews had the right and ability to supervise the infringing conduct. The court noted that Perfect 10 apparently had not appealed the dismissal of its vicarious infringement claim against Livewire at the pleadings stage because it had not mentioned Livewire in the sections of its brief devoted to its vicarious infringement claims. Nevertheless, to the extent Perfect 10 appealed the dismissal and its argument was not waived, the court held that the district court correctly dismissed the vicarious infringement claim against Livewire because Perfect 10 failed to adequately plead that Livewire exercised the requisite control over the infringing activity of its clients.²⁶⁶²

(o) Masck v. Sports Illustrated

In Masck v. Sports Illustrated,²⁶⁶³ the plaintiff owned the copyright in an action play photograph of football player Desmond Howard. Without the plaintiff’s permission, the

²⁶⁵⁸ Id. at 673.

²⁶⁵⁹ Id.

²⁶⁶⁰ Id.

²⁶⁶¹ Id. at 674.

²⁶⁶² Id.

²⁶⁶³ 2013 U.S. Dist. LEXIS 81677 (E.D. Mich. June 11, 2013).

photograph was uploaded for sale by a third party on the marketplace at Amazon.com. The plaintiff sued Amazon for contributory and vicarious liability and Amazon moved to dismiss the claims. The court denied Amazon's motion with respect to the claim of contributory liability, finding that Amazon had knowledge of the infringing activity because the plaintiff had requested Amazon to take down the infringing photograph. However, Amazon continued offer the photograph for sale in its marketplace after the requested removal, and the court concluded that such continued sale was a material contribution to infringement. The court rejected Amazon's reliance on the Sony case, finding the Sony rule to be applicable only to imputing culpable intent from the characteristics or uses of a distributed product. Here, there was no need to impute culpable intent because Amazon continued to offer the photo for sale on its website after receiving notice that it was infringing.²⁶⁶⁴

The court, however, granted Amazon's motion to dismiss with respect to the plaintiff's vicarious liability claim. The court agreed with Amazon's argument that it could not be expected to examine every product posted by a third party and determine whether or not it is infringing. The court held that the plaintiff's complaint, which alleged merely that Amazon had the right and ability to supervise the content of its web site, did not meet the pleading requirement as there were no factual allegations from which it could be determined that Amazon had the ability to supervise the infringing conduct. The plaintiff was required to put forth factual allegations that demonstrated Amazon could plausibly verify the copyright status of each and every piece of merchandise it listed from third party sellers. Failure to do so required dismissal of the claim.²⁶⁶⁵

(p) Rosen v. Global Net Access

In Rosen v. Global Net Access, LLC,²⁶⁶⁶ plaintiff Rosen discovered the unauthorized availability of his copyrighted photographs on a web site hosted by the defendant Global Net Access (GNAX), availablewallpapers.com. Rosen sent a letter by fax and email to the person named as designated copyright agent in GNAX's Acceptable Use Policy posted on its web site, stating that the material appearing on availablewallpapers.com infringed his copyrights. GNAX did not disable access to the allegedly infringing material until after Rosen filed a lawsuit against GNAX two months later, seeking to hold it liable for contributory infringement. GNAX asserted the Section 512(a) and 512(c) safe harbors as a defense.²⁶⁶⁷

The court noted that GNZ could be liable for contributory infringement if it knew or had reason to know of the infringing activity and materially contributed to the direct infringer's infringing activity. GNAX argued that reason to know was insufficient knowledge for contributory liability. The court rejected this argument, noting that if contributory liability could be based only on a finding of actual (i.e., subjective) knowledge, Section 512(c)(1)(A)(ii) of the

²⁶⁶⁴ Id. at *2-3, *20-22.

²⁶⁶⁵ Id. at *18-20.

²⁶⁶⁶ 2014 U.S. Dist. LEXIS 84560 (C.D. Cal. June 20, 2014).

²⁶⁶⁷ Id. at *2-6.

safe harbor (which looks to whether the service provider is “aware of facts or circumstances from which infringing activity is apparent”) would be superfluous, as there would be no reason to create a safe harbor for actions that do not create liability in the first place. The court found GNAX knew or should have known that Rosen’s copyrights were being directly infringed upon by a third party when it received Rosen’s DMCA notice by fax and email, and that GNAX materially contributed to direct copyright infringement by failing, after learning that such material was on its system, to purge specific infringing material until after it was served with the complaint.²⁶⁶⁸

The court further held that GNAX was not eligible for the DMCA safe harbors. Despite claiming to have collected some 750 DMCA takedown notices, GNAX did not timely produce evidence to demonstrate that it actually responded to allegations of copyright infringement in an expeditious manner. The court held that the failure to produce even a single record of a DMCA notification led it to an adverse inference that no working notification system existed. Thus, GNAX failed the threshold requirements of Section 512(i). The court also ruled that GNAX did not qualify for the Section 512(a) safe harbor, because it stored clients’ data on its servers, and its connection to its clients’ material was therefore not transient, as required by Section 512(a). Nor did GNAX qualify for the Section 512(c) safe harbor because it had failed to respond expeditiously to Rosen’s DMCA notice, not removing the allegedly infringing material until two months after receipt of Rosen’s notice. The court also ruled that Rosen was entitled to recover reasonable attorneys’ fees and costs, provided he filed a timely motion in support thereof.²⁶⁶⁹

(q) Capitol Records v. Escape Media

(For a discussion of contributory liability issues in this case, see Section III.C.1(c) above.)

(r) UMG Recording v. Escape Media

(For a discussion of contributory liability issues in this case, see Section III.C.1(d) above.)

(s) Fox Broadcasting v. Dish Network

(For a discussion of the court’s holding that Dish was not liable for contributory infringement by virtue of offering its Prime Time Anytime (PTAT) and Hopper Transfers services that enabled its subscribers to time shift and place shift Fox programming onto mobile devices, because such time shifting and place shifting was a fair use, see Section II.A.4(u) above.)

(t) Smith v. Barnesandnoble.com

(For a discussion of contributory liability issues in this case, see Section III.C.1(f) above.)

²⁶⁶⁸ Id. at *7-9.

²⁶⁶⁹ Id. at *11-14.

(u) **Hart v. Amazon.com, Inc.**

In this case, the plaintiff was the author of three books, one of which, titled *Vagabond Natural*, was posted for sale on Amazon.com without authorization by one of Amazon's third party agent sellers. The plaintiff sought to hold Amazon liable as a direct infringer for listing the title of the plaintiff's book on the site and as a vicarious and contributory for processing the sale of a counterfeit copy of the book. The court granted Amazon's motion to dismiss on the pleadings. With respect to the direct infringement claim against Amazon, the court noted that titles of books are not copyrightable.²⁶⁷⁰ With respect to the claims of vicarious and contributory liability, the court concluded that they must be dismissed because the plaintiff had failed to sufficiently allege a claim for direct copyright infringement against the third party seller. The plaintiff had alleged only that the third party seller unlawfully copied in its entirety his original work of *Vagabond Natural*, without providing any details that would support his claims for the alleged wrongful copying. The pleadings therefore failed to satisfy the Supreme Court's pleading requirements in *Iqbal* and *Twombly*. In addition, the court rejected the plaintiff's allegation that Amazon materially contributed to infringement because it processed an infringing sale of his book. The court ruled that a claim that Amazon processed a sale, even if it were aware of the infringement, was insufficient to support a claim for contributory infringement. However, the court granted the plaintiff, who was proceeding *pro se*, the opportunity to amend his complaint to overcome the noted defects in pleading.²⁶⁷¹

(v) **Tomelleri v. Zazzle, Inc.**

(For a discussion of contributory liability issues in this case, see Section II.G.1(b)(2)(i).m above.)

(w) **BMG v. Cox Communications**

The Proceedings in the District Court

In BMG Rights Management (US) LLC v. Cox Communications, Inc.,²⁶⁷² the plaintiff BMG Rights Management ("BMG")²⁶⁷³ sought to hold the defendants Cox Communications, Inc. and Cox Com, LLC ("Cox") contributorily and vicariously liable for alleged infringement of BMG's musical composition copyrights taking place over Cox's high-speed Internet service by virtue of users' use of the BitTorrent protocol to illegally upload and download music files. The details of

²⁶⁷⁰ Hart v. Amazon.com, Inc., 2015 U.S. Dist. LEXIS 164627 at *1-2, *7-8 (N.D. Ill. Dec. 6, 2015).

²⁶⁷¹ Id. at *10-15, 27.

²⁶⁷² 149 F. Supp. 3d 634 (E.D. Va. 2015), aff'd in part, rev'd in part & vacated in part, 881 F.3d 293 (4th Cir. 2018).

²⁶⁷³ A second plaintiff, Round Hill Music LP, also brought copyright infringement claims against the defendants, but the court ruled that the pertinent agreements submitted by Round Hill to establish its standing did not give it either co-ownership of the copyrights it asserted in the litigation or an exclusive license for any use of the copyrights, but rather established Round Hill as merely the provider of day-to-day administrative services with respect to the copyrights. The court therefore dismissed Round Hill's claims for infringement against the defendants. Id. at 648-53.

the facts of this case, as well as the court's ruling that Cox was not as a matter of law entitled to the Section 512(a) safe harbor under the DMCA, are discussed in Section III.C.6(b)(1)(i).h below.

After the close of discovery, Cox moved for summary judgment on five grounds: (1) whether there was evidence of direct infringement by third parties with respect to which Cox could be secondarily liable; (2) whether there was evidence of Cox's contributory infringement; (3) whether there was evidence of Cox's vicarious liability; (4) whether BMG failed to mitigate its damages; and (5) whether BMG's unclean hands barred its claims. For the reasons discussed below, the court found summary judgment inappropriate on the first four grounds, but ruled that Cox's defense of unclean hands failed as a matter of law.²⁶⁷⁴

Direct Infringement. The court turned first to whether there was adequate evidence of underlying direct infringement by third parties. It was undisputed that BMG had not identified a specific individual Cox account holder who utilized the BitTorrent protocol on Cox's Internet service to upload or download music files that infringed BMG's copyrights. Cox viewed this as a critical flaw in BMG's evidence and argued that BMG should have brought John Doe lawsuits and used subpoenas to establish at least one account holder as a direct infringer. Cox further argued that identifications by BMG's agent Rightscorp of IP addresses associated with Cox accounts was insufficient to establish that any infringing act was committed by a Cox account *holder* rather than some third party who tapped into the account holder's network, such as a neighbor accessing an unsecured wireless network or a babysitter at the account holder's home.²⁶⁷⁵

The court disagreed with Cox's articulation of what is required of a copyright owner in a secondary liability suit. First, imposing a rule that would require copyright owners to litigate John Doe lawsuits before bringing claims of secondary liability would undermine a key purpose of secondary liability claims. Where a widely shared service is used to commit infringement, it may be impossible to enforce copyright rights effectively against all direct infringers, making secondary liability against the distributor of the copying device or service the only practical alternative. Second, the court found that Cox's argument ignored the fact that BMG could establish direct infringement using circumstantial evidence giving rise to an inference that Cox account holders or other authorized users accessed its service to directly infringe. Here, there was adequate circumstantial evidence in the form of Rightscorp's identification of 2.5 million instances of Cox users making BMG's copyrighted works available for download, and Rightscorp itself had downloaded approximately 100,000 full copies of BMG's works using Cox's service. Accordingly, the court found that BMG had presented more than enough evidence to raise a genuine issue of material fact as to whether Cox account holders directly infringed its exclusive rights.²⁶⁷⁶

Cox argued that BMG could not rely solely on evidence compiled by Rightscorp because direct infringement requires a showing of volitional conduct by a third party, and BMG could not

²⁶⁷⁴ Id. at 639, 662-63.

²⁶⁷⁵ Id. at 663.

²⁶⁷⁶ Id.

rely on evidence of its own agent's volition. The court noted that other courts had routinely rejected the argument that evidence of infringement gathered by a copyright owner's investigative agent cannot be used to establish infringement. Where a copyright owner has not licensed its agent to authorize distribution or reproduction, the agent's downloading of the works is not authorized and thus does not run afoul of the general proposition that a copyright owner cannot infringe its own copyright. The court therefore concluded that the fact that Rightscorp caused over 100,000 downloads of the copyrighted works was sufficient to meet the volition requirement.²⁶⁷⁷

The court also found that Cox overstated the import of the distinction between infringement by the individual named on the account and infringement by other users with access to Cox service. Taking a scenario posed by Cox at oral argument, the court noted it is typical for each member of a multimember household to access the Internet via an agreement between Cox and one individual in the household. Evidence that any one of those users infringed would be sufficient, notwithstanding the fact that the individual's name did not appear on the bill. While identity is a key issue in many individual infringement suits, the court found that it has little relevance in a large-scale secondary liability suit. And Cox remained free to present evidence at trial that might weaken any inference raised by BMG's evidence of infringement, such as evidence of the prevalence of stolen access to wireless networks or what Cox believed to be Rightscorp's imprecise methods of identifying IP addresses engaged in allegedly infringing activity.²⁶⁷⁸

Whether the Distribution Right Includes "Making Available". Cox also argued that BMG's evidence of Cox account holders making copyrighted works available for download was insufficient to show infringement of the distribution right. Cox asserted that BMG must show actual dissemination of the copyrighted works and that BMG had failed to do so. BMG responded that the Fourth Circuit in the Hotaling case²⁶⁷⁹ had found that mere "making available" of a copyrighted work is sufficient to violate the distribution right, and that even if an actual distribution is required, there was sufficient evidence to establish infringement of its distribution right.²⁶⁸⁰ The court rejected BMG's reading of Hotaling, noting that Hotaling ruled that a party must show that an unlawful copy was "disseminated" to the public. The Fourth Circuit's specific holding that the plaintiffs established a distribution from the library under the particular facts of that case was driven by equitable concerns rather than an analysis of the statute – specifically, the copyright holder could not have been expected to be able to prove particular instances of use by the public when the proof was impossible to produce because the infringing library had not kept records of public use.²⁶⁸¹

²⁶⁷⁷ Id. at 664.

²⁶⁷⁸ Id.

²⁶⁷⁹ Hotaling v. Church of Jesus Christ of Latter-Day Saints, 118 F.3d 199 (4th Cir. 1997).

²⁶⁸⁰ Cox, 149 F. Supp. 3d at 664-65.

²⁶⁸¹ Id. at 665.

The district court concluded that, although some courts have construed Hotaling broadly and held that making works available via file-sharing is distribution, the general rule, supported by the great weight of authority, is that infringement of the distribution right requires an actual dissemination of either copies or phonorecords. The district court therefore joined those courts and held that Hotaling did not announce a rule of general applicability, but instead articulated a principle that applies only in cases where it is impossible for a copyright owner to produce proof of actual distribution. The court found that its reading of Hotaling was also consistent with the plain meaning of the statute. Congress provided a list in Section 106(3) of specific transactions that consummate a distribution: a transfer of a work to the public by sale or other transfer of ownership, or by rental, lease, or lending. Missing from the list is an *offer* to sell, transfer, rent, lease or lend a work.²⁶⁸²

The court rejected BMG's argument that the definition of "publication" in Section 101 supports a broader reading of the distribution right. That definition provides that the offering to distribute copies of phonorecords to a group of person for purposes of further distribution constitutes publication. The court noted that, although it is clear from the definition that all distributions are publications, the inverse is not true. The "offering to distribute" language forms an additional category of publications that are not distributions. The court therefore concluded that Section 101 provided no support for BMG's "making available" theory.²⁶⁸³

The court rejected three additional arguments by BMG for its "making available" theory. First, BMG asserted that "making available" is the view of definitive treatises. The court noted such assertion is not correct – there is a split in the academic debate, with Professors Menell and Nimmer advocating for a "making available" right and Professors Patry and Goldstein advocating for actual distribution. The court noted it would leave any further debate to academia. Second, BMG argued that interpreting the distribution right broadly was essential to comport with U.S. obligations under the WIPO Copyright Treaty. The court noted that while the WIPO Treaty does recognize a "making available" right, the treaty is not self-executing and lacks any binding legal authority separate from its implementation through the Copyright Act, the plain language of which the court had construed not to afford a "making available" form of the distribution right. Third, BMG cited a letter written by Marybeth Peters, the former Register of Copyrights, that embraced a "making available" reading of the statute. The court summarily dismissed this argument, noting that the opinions expressed in the letter had no controlling weight and the court would not consider them.²⁶⁸⁴

Although siding with Cox on the "making available" issue, the court noted that Cox made two additional arguments regarding the contours of the distribution right that it did not accept. First, Cox contended that the phrase "copies or phonorecords" covers only tangible, material objects and the distribution right is not infringed by electronic, rather than physical, transfers. Second, Cox argued that the transactional language in the statute – "by sale or other transfer of

²⁶⁸² Id. at 666.

²⁶⁸³ Id. at 667-68.

²⁶⁸⁴ Id. at 668.

ownership, or by rental, lease, or lending” – requires that there be a consummated “transfer” of the a copy or phonorecord and that there was no evidence of such a transfer in this case. The court rejected these arguments, citing cases holding that any object in which a sound recording can be fixed is a “material object,” including electronic files. The court further ruled that, not only can electronic files be “material objects,” but transferring files using the BitTorrent protocol satisfies the transactional element of distribution. While BitTorrent transfers do not fit within the ordinary conception of a “transfer of ownership” because the transferor retains his or her own copy of the file, the court ruled that what matters is that when the transaction is completed, the distributee has a material object, not whether the transferor gives up his or her own.²⁶⁸⁵

BMG contended that, even under a standard requiring it to shown an actual dissemination of a copyrighted work to establish direct infringement, it had produced more than enough evidence to show actual dissemination. First, Rightscorp identified Cox subscribers sharing torrents that Rightscorp had also found on torrent indexing web sites. Because each torrent contained a unique hash, BMG argued those Cox users must have downloaded the torrents at some point. Second, Rightscorp downloaded over 700,000 copies of copyrighted works from Cox subscribers using Cox’s Internet service and 100,000 of those copies were of the works at issue in the case. Third, Rightscorp asserted it identified 2.5 million instances in which Cox users made available the copyrighted works for downloading. BMG argued that even if this “making available” evidence was not direct evidence of distribution, it was circumstantial evidence that the works were in fact downloaded given the way the BitTorrent protocol operates. The court agreed, finding that BMG had demonstrated that there was a genuine issue of material fact as to whether its distribution right was directly infringed.²⁶⁸⁶

Contributory Infringement. The court began its analysis of the contributory infringement issue by stating the standard of contributory infringement from the Fourth Circuit’s CoStar case: a contributory infringer is one who with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another.²⁶⁸⁷ BMG claimed that Cox knew, had reason to know, or was willfully blind to its users’ infringement and materially contributed to that infringement. Cox contended, first, that only an inducement theory of contributory infringement survived the Supreme Court’s decision in Grokster when it said that “[o]ne infringes contributorily by intentionally inducing or encouraging direct infringement.”²⁶⁸⁸ The district court rejected this reading of Grokster, finding that Grokster clarified the scope of inducement, but did not explicitly or implicitly reject a material contribution theory of liability.²⁶⁸⁹ The court

²⁶⁸⁵ Id. at 669-70.

²⁶⁸⁶ Id. at 670.

²⁶⁸⁷ Id. (citing CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 550 (4th Cir. 2004)).

²⁶⁸⁸ Cox, 149 F. Supp. 3d at 671 & n. 24 (quoting Metro-Goldwin-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005)).

²⁶⁸⁹ Cox, 149 F. Supp. 3d at 671 (citing Perfect 10, Inc. v. Giganews, Inc., 2014 U.S. Dist. LEXIS 183590 at *6 (C.D. Cal. Nov. 14, 2014), rejecting the same argument).

also found it persuasive that in the wake of Grokster courts had continued to articulate both inducement and material contribution theories of contributory infringement.²⁶⁹⁰

Cox argued that even if a “material contribution” theory survived Grokster, BMG could not succeed because there was no evidence that Cox had knowledge of infringing activity.²⁶⁹¹ The court noted the knowledge requirement can be met by a showing of actual or constructive knowledge or by evidence that a defendant took deliberate actions to willfully blind itself to specific infringing activity. The court observed that, although a couple of decisions by the Ninth Circuit had abandoned constructive knowledge in the online context and instead required plaintiffs to establish actual knowledge of specific acts of infringement, absent any indication from the Fourth Circuit to the contrary, the court would decline to alter the contributory infringement standard, including its alternative constructive knowledge and willful blindness bases.²⁶⁹²

BMG asserted Cox had knowledge of its users’ infringing activity because Rightscorp sent Cox more than two million infringement notices pertaining to its copyrighted works. The court noted that, despite Cox’s arguments to the contrary, DMCA-compliant notices are evidence of knowledge. The court further observed, however, that the case presented an unusual fact pattern, because it was undisputed that Cox never received Rightscorp’s notices related to BMG’s copyrights during the period covered by the complaint since Cox began blocking Rightscorp’s notices at the server level in 2011. Cox contended that even had Cox received the notices, they were not evidence of knowledge because they were deficient. The court rejected this, noting that Cox asserted that if Rightscorp had only agreed to delete the settlement language from the notices, they would have been forwarded to Cox account holders. The court therefore held that, at the present stage of the litigation, viewing the evidence in the light most favorable to BMG, a reasonable trier of fact could conclude that had Cox received the notices, they would be evidence of infringing activity.²⁶⁹³

BMG argued that Cox’s unreasonable decision not to receive Rightscorp’s notices gave Cox reason to know of the infringing activity. First, BMG claimed that when Cox refused to forward its notices, it gave Cox access to a searchable and sortable “dashboard” that contained all of the information pertaining to the alleged infringements occurring at each IP address. Although Cox received an email from Rightscorp with instructions on how to access the dashboard, Cox maintained it never in fact accessed the dashboard and thus it could not have been a source of knowledge. Second, BMG asserted that after Cox blocked Rightscorp’s notices, Rightscorp sent emails to a manager of Cox’s abuse group and Cox’s in-house privacy counsel identifying IP addresses with a significant amount of infringing activity. Finally, BMG pointed to

²⁶⁹⁰ Cox, 149 F. Supp. 3d at 671.

²⁶⁹¹ The court noted that, because Cox had not raised BMG’s ability to establish the “material contribution” element until its reply brief, the court would not reach the issue of whether there was sufficient evidence of Cox’s contribution to the alleged infringement. Id. at 671 n.25.

²⁶⁹² Id. at 671 & n.26.

²⁶⁹³ Id. at 671-72 & n.27.

email statements by members of Cox’s abuse group that described specific customers with phrases like “habitual abuser” or “well aware of his actions.” The court found such emails showed Cox employees discussing specific interactions with individual Cox account holders regarding what Cox employees believed was specific infringing activity. Even if the emails would not be sufficient standing alone to establish knowledge, they strengthened the inference that Cox’s knowledge of infringement went beyond the mere possibility that its service was being used for infringement. Considering all of the foregoing together, the court ruled that a reasonable jury could conclude that Cox’s refusal to accept Rightscorp’s notices was unreasonable and that additional notice provided to Cox gave it reason to know of the allegedly infringing activity on its network.²⁶⁹⁴

With respect to willful blindness, the court noted the governing standard is whether the defendant was aware of a high probability of the fact in dispute and consciously avoided confirming that fact. Mere negligence or recklessness is insufficient – there must be evidence that the defendant took deliberate actions to avoid confirming a high probability of wrongdoing. The court noted a number of competing inferences that a jury could reasonably draw from the facts of the case with respect to willful blindness. BMG argued that Cox’s failure to terminate repeat infringers from its service and its deliberate avoidance of Rightscorp’s notices established its willful blindness. Cox pointed to actions it did take when it received what it considered proper infringement notices, including forwarding hundreds of thousands of infringement notices annually, working with account holders to identify and stop the activities causing the notices, and suspending and when necessary terminating account holders. The court observed that this generalized evidence that Cox did not always turn a blind eye to infringement did not mean that it had never done so. Cox also argued that because it offered to work with Rightscorp to remove improper language from its notices, there was no evidence it was deliberately avoiding knowledge of illegal activity. The court observed that, while this would certainly be a reasonable inference for a jury to draw, it was not the only inference available. The court noted that a jury could also justifiably draw an inference suggested by BMG that Cox was a company unhappy with the burdens of complying with the DMCA and was using the settlement offers in Rightscorp’s notices as a red herring to distract from its goal of reducing the number of infringement notices Cox received.²⁶⁹⁵

Vicarious Infringement. The court began its vicarious infringement analysis by quoting the Fourth Circuit’s standard, which requires a showing that the defendant possessed the right and ability to supervise the infringing activity and possessed an obvious and direct financial interest in the exploited copyrighted materials. The court elaborated that under Grokster, the first element requires that the defendant declined a right to stop or limit the direct infringement. The court noted that Cox had the contractual right to condition the availability of its Internet access to users who do not use that service to violate copyrights. If users listened when Cox exercised that power, infringement stopped. If users did not and Cox terminated them, that also stopped or at least limited infringement. In addition to its legal control, the court observed that

²⁶⁹⁴ Id. at 672 & n.28.

²⁶⁹⁵ Id. at 673.

Cox also had the practical ability to stop or limit infringement. There could not be any serious dispute that Internet service was an essential component of the infringing activity alleged by BMG, as file-sharing programs were completely dependent on the Internet to facilitate the download and upload of files. It was therefore a reasonable inference that the result of Cox exercising its ability to suspend or terminate account holders would stop or limit infringement.²⁶⁹⁶

Cox argued that a mere legal right to stop or limit infringing activity by terminating accounts was insufficient, and that there must also be evidence that Cox's current architecture would allow it to exercise physical control over the infringing activity. Cox reasoned that the provision of general Internet service is much different from the swap market in the Ninth Circuit's Fonovisa case (cited by BMG), where the defendant also controlled the access of its customers to the swap meet area. The court was not persuaded, citing a dissent by Judge Kozinski in the Ninth Circuit's Perfect 10 v. Visa case observing that physical control over the infringing activity is one way to stop infringers, but it is not the only way, and that withdrawing crucial services can be just as effective. In sum, the court concluded that because Cox had a contractual relationship with its users that gave it the legal right to withhold service in the face of infringing conduct, and Cox had the practical ability to stop or limit infringement by withdrawing a crucial service to the infringements, that was sufficient to raise a genuine issue of material fact as to whether BMG could establish the first element of its vicarious liability claim.²⁶⁹⁷

Turning to the direct financial interest prong, the court noted that it requires a causal relationship between the infringing activity and any financial benefit a defendant reaps, regardless of how substantial the benefit is in proportion to a defendant's overall profits. Financial benefit can be shown by evidence that the availability of infringing material acts as a draw for customers, and the draw of infringement need not be the primary, or even a significant draw – rather, it need be only a draw. While the draw need not be significant, the requisite causal connection must be between the infringing activities *at issue in the case* and a direct financial benefit to the defendant. The court noted that, because Cox charged the same flat monthly fees to its users whether they used Cox's service for infringing or non-infringing purposes, receipt of such fees would be evidence of direct financial benefit only if some portion of those fees was generated from subscribers that were drawn to Cox's service at least in part because of the infringing activity alleged. Without that evidence, the requisite causal connections between the benefit and the infringing activity would not be established.²⁶⁹⁸

BMG offered evidence of the draw of infringing activity in the form of an expert survey of Cox subscribers concluding that 16% of subscribers downloaded or uploaded free digital music through sites such as ThePirateBay, KickAssTorrents, and Torrentz, and of that 16%, 70% characterized the ability to do so as a reason they subscribed to Cox. The court observed that, while such evidence was hardly overwhelming, it was not clearly insufficient to satisfy the legal

²⁶⁹⁶ Id. at 674.

²⁶⁹⁷ Id. at 674-75.

²⁶⁹⁸ Id. at 675-76.

standard. Viewing the evidence in the light most favorable to BMG, the court found that a reasonable trier of fact could conclude that some percentage of Cox customers were drawn to Cox's Internet service at least in part to download music, including BMG's copyrighted works, using the BitTorrent protocol.²⁶⁹⁹

Mitigation of Damages. Cox raised BMG's alleged failure to mitigate its damages as a ground for summary judgment – specifically, BMG's failure to mitigate by declining to modify Rightscorp's infringement notices and by failing to pursue other source of infringement. The court observed that district courts are divided on the legal question of whether a plaintiff's election of statutory damages invalidates a failure-to-mitigate defense. The court agreed with those courts holding that it does not, because a plaintiff's actual damages are a relevant consideration in determining statutory damages under the Copyright Act. The court concluded that, to the extent failure to mitigate damages is applicable to the award of statutory damages, a genuine issue of material fact remained as to whether BMG in fact failed to mitigate its damages.²⁷⁰⁰

Unclean Hands. Finally, Cox contended that BMG's claims were barred by unclean hands on two grounds. First, Cox argued that BMG failed to supervise its agent Rightscorp and cast a blind eye toward Rightscorp's extortionate scheme to profit from threats that Cox would cut off Internet service if Cox's subscribers did not pay Rightscorp. The court noted that the only conduct by Rightscorp with a direct nexus to the litigation was the inclusion of settlement offers in its notices sent to Cox subscribers. The court found the notices were not evidence of misconduct rising to the level of fraud, deceit, unconscionability or bad faith. Cox's remaining allegations, which amounted to general attacks on Rightscorp's business model, were all directed toward Rightscorp's treatment of third parties. The court found that none of those alleged practices resulted in any injury to Cox or any Cox customer and thus could not form the basis of an unclean hands defense.²⁷⁰¹

Second, Cox argued that BMG was not entitled to relief because Rightscorp downloaded thousands of sound recordings and there was no evidence that Rightscorp had authorization to do so from the owners of the sound recording copyrights (as opposed to authorization from BMG, which owned the musical composition copyrights). The court rejected this, citing a statement in the Nimmer treatise that use of undercover investigators and the like to ferret out infringement is routine, and provides no defense. The court further observed that the downloading did not personally injure Cox, so the conduct could not be used as the basis of an unclean hands defense. Accordingly, the court ruled that Cox's unclean hands defense failed as a matter of law.²⁷⁰²

²⁶⁹⁹ Id. at 676.

²⁷⁰⁰ Id. at 676-77.

²⁷⁰¹ Id. at 677-78.

²⁷⁰² Id. at 678.

In view of its rulings, the court allowed the case to proceed to trial before a jury. On Dec. 17, 2015, the jury returned a verdict finding Cox liable for contributory infringement and finding that Cox's infringements were willful, but finding Cox not liable for vicarious infringement. The jury awarded BMG \$25,000,000 in statutory damages, or approximately \$18,000 per infringed work.²⁷⁰³

The Post-Trial Rulings

After the verdict, Cox moved for judgment as a matter of law or, in the alternative, a new trial, and BMG moved for judgment as a matter of law on its claim of vicarious infringement as well as for permanent injunctive relief.²⁷⁰⁴ The court denied all post-trial motions for the following reasons.

Cox argued that BMG had not adequately established direct infringement by Cox's users for which Cox could have secondary liability. Cox relied in part on extensive evidence it submitted pertaining to the unreliability of Rightscorp's software in detecting infringing activity, in addition to the fact that Rightscorp had not used version control software and therefore did not have a complete historical version of Rightscorp's source code for any period of time relevant to the suit. But the court noted that such evidence had not gone unanswered by BMG, including testimony by BMG's expert that a comparison of a partial copy of a 2013 version of the source code she had retained in her files against the 2015 version of the code introduced at trial revealed no significant differences in the code's core functionalities. And the court noted that BMG's experts had responded at length to the deficiencies in the Rightscorp infringement data identified by Cox.²⁷⁰⁵

Cox further argued that BMG's distribution claim failed because the only evidence of peers connected to Cox IP addresses distributing BMG's works was to Rightscorp, and because Rightscorp was acting as an authorized agent of BMG, that evidence could not be the basis of BMG's distribution claim. The court rejected this argument, noting that other courts had consistently relied upon evidence of downloads by a plaintiff's investigator to establish both unauthorized copying and distribution of a plaintiff's work.²⁷⁰⁶

Cox also argued that it had rebutted BMG's claim there was substantial indirect evidence of distribution by Cox users over its network, by virtue of the fact that Rightscorp failed to record the "unchoke" signal generated in peer communications under the BitTorrent protocol.

²⁷⁰³ See Eriq Gardner, "Music Publisher Gets \$25 Million Jury Verdict Against Cox in Trailblazing Piracy Case," available as of Dec. 17, 2015 at www.billboard.com/articles/business/6813610/bmg-25-million-jury-verdict-cox-piracy. The jury's verdict form may be found at www.documentcloud.org/documents/2648509-BMG-Verdict.html.

²⁷⁰⁴ BMG Rights Mgmt. (US) LLC v. Cox Comm'ns, Inc., 199 F. Supp. 3d 958 (E.D. Va. 2016), aff'd in part, rev'd in part & vacated in part, 881 F.3d 293 (4th Cir. 2018).

²⁷⁰⁵ Id. at 969-70.

²⁷⁰⁶ Id. at 972.

Specifically, following the handshake signal establishing communication between two peers in a BitTorrent exchange, the requesting peer sends an “unchoke” message to the peer with the file to begin the uploading process. Under certain circumstances, a peer may remain “choked” and not send the requested pieces of the file. Rightscorp’s software did not take the additional step of recording the choke/unchoke interaction to confirm that a peer was set to share a given file. Based on this failure, Cox argued that Rightscorp’s 1.8 million observations of peers connected through Cox IP addresses indicating they had a complete BMG work to share were not confirmed offers to upload, and if true, the observations were not even circumstantial evidence of distribution. The court noted that Cox had presented no testimony that choking is a common occurrence, and the evidence at trial indicated the opposite. The court therefore found the evidence of Rightscorp’s 1.8 million observations, together with evidence of Cox IP addresses uploading more than 100,000 copies of BMG’s works, to be sufficient for a reasonable jury to find Cox users violated BMG’s reproduction and distribution rights.²⁷⁰⁷

With respect to Cox’s challenge to BMG’s contributory infringement claim, the court noted that Cox and BMG disagreed on the state of the law of contributory infringement after the Supreme Court’s decision in Grokster. The court observed that throughout the litigation, it had taken the position that the Supreme Court’s Sony decision is not the broad bar to secondary liability that Cox argued it to be. Rather, the court reiterated that it read Sony as precluding the imputation of fault based solely on the design or distribution of a product capable of substantial lawful use, which the distributor knows is in fact used for infringement. Had that been BMG’s claim, the court observed that it would have failed, because Cox’s mere provision of Internet access that supplies the means to infringe could not, standing alone, constitute contributory infringement under Sony.²⁷⁰⁸

But the court noted that was not the claim BMG made. BMG’s claim went beyond design choice or the mere provision of a service and therefore went beyond Sony. Instead, BMG focused on Cox’s conduct in relation to the operation of its service. Specifically, BMG claimed that Cox ignored specific notices of infringing activity and continued to provide material support to its users’ infringement of BMG’s works despite its ability to suspend or terminate customers with the push of a button. Such claim was possible here because, unlike in Sony, Cox maintained an ongoing relationship with users of its service, and an ongoing relationship between a defendant and direct infringers presents a potential for culpability quite beyond distribution or design. The court emphasized that the distinction it was drawing was not between products and services, nor was it that whenever a defendant is involved beyond manufacture and distribution of a product or service, Sony has no application. Rather, Sony provides a safe harbor from imputing culpability for mere distribution of a product or service that has commercially significant lawful uses and in doing so ensures that copyright holders cannot gain effective control over the sale of that item by way of indirect liability. But in the court’s view, Sony did not immunize a defendant from liability when it maintains an ongoing relationship with users, knows

²⁷⁰⁷ Id. at 971-73.

²⁷⁰⁸ Id. at 975.

of specific infringement, and continues to provide material assistance in the face of that knowledge.²⁷⁰⁹

Cox further argued that if Sony did not provide immunity, under the Supreme Court's Grokster decision BMG's only path to liability was through an inducement claim, in view of the Supreme Court's statement in Grokster that "[o]ne infringes contributorily by intentionally inducing or encouraging direct infringement"²⁷¹⁰ The district court disagreed, citing passages in the Grokster opinion noting that Sony was never meant to foreclose rules of fault-based liability derived from the common law and did not displace other theories of secondary liability. Accordingly, the court concluded that Grokster did not suggest that a court must find inducement in order to impose contributory liability. The court had therefore permitted BMG to go forward on its claims and attempt to prove Cox had knowledge that users of its Internet service were infringing BMG's copyrights and that Cox materially contributed to that infringement.²⁷¹¹

The court charged the jury that BMG had to establish that Cox knew or should have known of the direct infringing activity by users of its Internet service and that knowledge could be established if Cox acted with willful blindness – i.e., it was aware of a high probability that Cox users were infringing BMG's copyrights but consciously avoided confirming that fact. The court noted that, although the significant amount of evidence of Cox's general knowledge of infringement on its network was not sufficient standing alone for liability, it provided the backdrop for Cox's decision to continuously ignore and take no action in response to the 1.8 million notices, weekly letters, and dashboard from Rightscorp. The court noted there was also evidence that Cox had configured its graduated response system in such a way as to reduce both the total number of notices that entered the system and the amount of customer-facing action that it took. Moreover, internal communications, which were admitted over Cox's objection, signaled that Cox's decision not to process Rightscorp's notices may have been due to more than just the presence of the settlement language and instead reflected a general disdain for any enforcement responsibilities.²⁷¹² The court therefore ruled that the jury could reasonably conclude that Rightscorp captured infringing activity on Cox's network, and that had Cox received the notices they would have satisfied the knowledge requirement.²⁷¹³

The court quickly dismissed Cox's challenge to the material contribution requirement, finding that it need not address material contribution at length in view of its rejection of rejection of Cox's Sony argument.²⁷¹⁴ Said the court, "There can be no question that the

²⁷⁰⁹ Id. at 975-76 & n.16.

²⁷¹⁰ Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005).

²⁷¹¹ Cox, 199 F. Supp. 3d at 976-77.

²⁷¹² Id. at 977-78. The court observed that Jason Zabek, the former head of Cox's Abuse Group, summed up Cox's general sentiment toward its obligations best in an email exclaiming: "f the dmca!!!" Id. at 967.

²⁷¹³ Id. at 979.

²⁷¹⁴ Id.

provision of high-speed internet service materially contributes to infringement via BitTorrent and that Cox had the means to withhold that assistance upon learning of specific infringing activity.”²⁷¹⁵

With respect to Cox’s motion for a new trial, the court rejected a number of challenges made by Cox to the instructions given to the jury with respect to direct infringement, contributory infringement, statutory damages, and the relevance of the DMCA, and with respect to a finding of spoliation that the magistrate judge in the case had made during discovery.²⁷¹⁶ The court also rejected several challenges by Cox to various of its evidentiary rulings.²⁷¹⁷

Turning to BMG’s motion for judgment as a matter of law on its vicarious infringement claim, the court found the jury had a substantial basis on which to conclude that Cox did not maintain an obvious and direct financial interest in the infringement of BMG’s works on its network. BMG relied heavily on a survey conducted by its expert purporting to show that nearly 10% of Cox subscribers subscribed to Cox’s Internet service in order to use BitTorrent sites and share music. But Cox had effectively undermined numerous aspects of the survey, including the methodology used and the conclusions drawn. The court concluded the jury was well within its right to give the survey very little, if any, weight at all. Moreover, BMG’s reliance on internal Cox documents referencing the fact that a certain percentage of its subscribers used peer-to-peer software to acquire music did not, without more, establish that those same subscribers were drawn to Cox’s service on that basis or that Cox had a financial interest in that activity.²⁷¹⁸

Finally, the court turned to BMG’s motion for a permanent injunction. At the outset, the court noted that BMG’s brief in support of an injunction relied heavily on a statement of fact that was not true. Specifically, BMG alleged that, following the jury verdict, Cox had continued to ignore Rightscorp’s notices on its network. In fact, Cox had provided notice to BMG shortly after trial that Rightscorp’s notices were no longer blacklisted. Despite that, neither Rightscorp nor BMG submitted any infringement notifications to Cox. After discovering its gaffe, BMG’s counsel notified the court by letter but asserted that its error did not lessen the ongoing harm to BMG. The court observed that BMG’s error highlighted the difficulty of fashioning an injunction in which Rightscorp would be an essential entity.²⁷¹⁹

The court found even greater pause from the lack of detail in BMG’s proposed injunction. Under BMG’s proposed injunction, Cox would be “enjoined from knowingly and materially contributing to the unauthorized copying, uploading, downloading, transmitting, or distributing by others using its network of any musical composition in which BMG owns or controls an

²⁷¹⁵ Id. The court similarly quickly disposed of Cox’s challenge to the jury’s finding on willfulness, noting there was sufficient evidence for the jury to find Cox was aware of the infringing activity and that it acted recklessly or with deliberate disregard. Id. at 981.

²⁷¹⁶ Id. at 981-87.

²⁷¹⁷ Id. at 987-92.

²⁷¹⁸ Id. at 992.

²⁷¹⁹ Id. at 993-94.

exclusive right under the United States Copyright Act.”²⁷²⁰ The court noted that was essentially an order to Cox not to violate the law which failed F.R.C.P. 65(d)’s requirement that an injunction state its terms specifically and describe in reasonable detail the act or acts restrained or required. The court found the proposed injunction severely lacking in conduct-based instruction.²⁷²¹ The only conduct (as opposed to a legal standard) identified was that Cox was to notify subscribers of certain information within BMG’s notices within two days of receipt and then, within seven days, Cox was required to “inform BMG in writing of (a) the identity of and contact information (including, if available, email address, postal address, and telephone number) of the Cox subscriber assigned the IP address identified in the Notice at the date and time specified in the Notice and (b) the action Cox has taken to prevent or limit further infringement of the BMG Copyrighted Work identified in the Notice.”²⁷²²

The court noted BMG had no suggestions for what it meant to require Cox “to prevent or limit further infringement.” Picking two verbs without any additional detail as to what they might mean in practice was wholly insufficient.²⁷²³ The court further noted that Cox identified only a handful of the multitudes of questions that this language would require answering:

Is Cox required to suspend accused infringers, or simply terminate them upon one notice, or after the second notice? What if BMG sends ten notices for one IP address in one hour, or one minute? If the injunction requires termination of “repeat” infringing subscribers in appropriate circumstances, when is a subscriber a “repeat” infringer, and what are the “appropriate circumstances” for termination? Does the order permit or require suspension before termination? Can Cox warn the account holder first? Is Cox permitted to give customers an opportunity to respond to the accusations against them, or is it required to terminate accused infringers and provide them no redress? If the subscriber denies the accusation, what process will exist to adjudicate the accusation by BMG? Can Cox implement a counter-notice process such as the DMCA provides for storage providers? What if, for example, the subscriber’s computer was infected with malware, the user’s network password was stolen, or a neighbor or guest accessed the user’s account?²⁷²⁴

The court also expressed concern that, in addition to asking the court to set Cox’s business practices, injunctive relief would almost certainly require oversight of Rightscorp’s practices as well. Yet the proposed injunction was entirely silent on that front. BMG cited numerous cases in which it asserted courts had imposed similarly broad injunctions in analogous cases. The court found those cases analogous to the extent they involved peer-to-peer file sharing, but noted that none involved an intermediary in Cox’s position, and instead highlighted

²⁷²⁰ Id. at 994.

²⁷²¹ Id. at 994.

²⁷²² Id.

²⁷²³ Id. at 995.

²⁷²⁴ Id.

the need for care in crafting injunctions to reach only the illegality and to preserve, to the extent possible, legal uses.²⁷²⁵

The court was also concerned about the provisions of the injunction requiring Cox to hand over the identity, email address, mailing address, and telephone number of every subscriber that BMG identified. When asked at oral argument, BMG’s counsel conceded that the information would be given to Rightscorp but insisted that there would be the “usual brakes” on someone abusing that sort of information. The court observed that what those “usual brakes” were was not clear, but what was clear was that none of them appeared in the proposed injunction. The court also found that the balance of hardships and the public interest did not support entering an injunction. For its part, BMG had waited years to bring the lawsuit. The court noted it did not question the harm BMG suffers each time a work becomes available on BitTorrent, but BMG had not sufficiently articulated how maintaining its years-long status quo outweighed the burden it wished to place on Cox.²⁷²⁶

Finally, BMG had not shown that it was possible to craft an injunction that would not disserve the public interest. The court noted the relief requested would have a substantial spillover effect far beyond the parties to the lawsuit at hand. While there was without a doubt a significant public benefit in reducing copyright infringement, BMG had not demonstrated to the court’s satisfaction that such a reduction in this instance would not come at the expense of other nontrivial interests, including privacy and access to the Internet. Accordingly, the court denied the motion for a permanent injunction.²⁷²⁷

In a subsequent order, the court awarded BMG \$8,383,468.06 in attorneys’ fees.²⁷²⁸

The Fourth Circuit’s Decision

On appeal, the Fourth Circuit reversed in part and remanded for a new trial based on erroneous jury instructions on contributory infringement.²⁷²⁹ Cox argued that the court’s jury instructions on contributory infringement were erroneous because they did not instruct the jury that Cox could not be held liable for contributory infringement under the Supreme Court’s Sony case if its technology was capable of substantial noninfringing use. The court rejected this argument. The Fourth Circuit noted that, although a few courts initially interpreted Sony as Cox was arguing, the Supreme Court in Grokster rejected this broad reading.²⁷³⁰ The Fourth Circuit pointed out that the Supreme Court stated in Grokster that “Sony barred secondary liability

²⁷²⁵ Id. at 995-96.

²⁷²⁶ Id. at 996-97.

²⁷²⁷ Id. at 997-98.

²⁷²⁸ BMG Rights Mgmt. (US) LLC v. Cox Communs., Inc., 234 F. Supp. 3d 760 (E.D. Va. 2017).

²⁷²⁹ BMG Rights Mgmt. (US) LLC v. Cox Communs., Inc., 881 F.3d 293 (4th Cir. 2018). The Fourth Circuit affirmed the court’s ruling that Cox was not entitled to a DMCA safe harbor. A discussion of that portion of the decision is set forth in Section III.C.6(b)(1)(i).h below.

²⁷³⁰ Id. at 305-06.

based on *presuming or imputing intent* to cause infringement solely from the design or distribution of a product capable of substantial lawful use, which the distributor knows is in fact used for infringement” and further explained that, under Sony, intent to infringe will not be presumed from “the equivocal conduct of selling an item with substantial lawful as well as unlawful uses,” even when the seller has the “understanding that some of [his or her] products will be misused.” The fact that a product is “capable of substantial lawful use” does not, however, mean the “producer can never be held contributorily liable.”²⁷³¹

The Fourth Circuit found that the same flaw infected Cox’s related argument that the district court erred in refusing to instruct the jury that it is not a material contribution to provide a product or service that is capable of substantial noninfringing uses. As the Supreme Court explained in Grokster, reversal was required because the Ninth Circuit had read Sony’s limitation to mean that whenever a product is capable of substantial lawful use, the producer can never be held contributorily liable for third parties’ infringing use of it. In fact, providing a product with substantial noninfringing uses can constitute a material contribution to copyright infringement.²⁷³² The Fourth Circuit stated that Grokster makes clear what matters is not simply whether the product has some or even many noninfringing uses, but whether the product is distributed with the *intent* to cause copyright infringement,²⁷³³ citing the statement in Grokster that “Sony’s rule limits imputing *culpable intent* as a matter of law from the characteristics or uses of a distributed product.”²⁷³⁴ The Fourth Circuit therefore ruled that, because Cox’s requested instruction misstated the law, the district court did not err in refusing to give it.²⁷³⁵

Cox further challenged the district court’s instructions that the jury could impose liability for contributory infringement if the jury found Cox knew or should have known of such infringing activity.²⁷³⁶ The Fourth Circuit agreed that in so instructing the jury, the district court erred, citing Grokster’s statements that “[o]ne infringes contributorily by *intentionally* inducing or encouraging direct infringement” and that the requisite intent may be presumed according to the “rules of fault-based liability derived from the common law.”²⁷³⁷ The most relevant of the common law rules is that if a person “knows that the consequences are certain, or substantially certain, to result from his act, and still goes ahead, he is treated by the law as if he had in fact desired to produce the result.”²⁷³⁸ Similarly, when a person sells a product that has lawful uses, but with the knowledge that the buyer will in fact use the product to infringe copyright, he will

²⁷³¹ Id. at 306 (quoting Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 545 U.S. 913, 932-34 (emphasis added)).

²⁷³² Cox, 881 F.3d at 306.

²⁷³³ Id.

²⁷³⁴ Grokster, 545 U.S. at 934 (emphasis added).

²⁷³⁵ Cox, 881 F.3d at 307.

²⁷³⁶ Id.

²⁷³⁷ Id. (quoting Grokster, 545 U.S. at 934-35 (emphasis added)).

²⁷³⁸ Cox, 881 F.3d at 307 (quoting Restatement (Second) of Torts § 8A cmt. B (1965)).

be liable. The Fourth Circuit observed that these principles apply equally in cases, like this one, that involve subscription services or rentals rather than one-time sales.²⁷³⁹

The court noted it is well-established that one mental state slightly less demanding than actual knowledge – willful blindness – can establish the requisite intent for contributory copyright infringement, because the law recognizes willful blindness as equivalent to actual knowledge. But the court observed that whether other mental states – such as negligence (where a defendant “should have known” of infringement) – can suffice to prove contributory infringement presented a difficult question. It ultimately agreed, for several reasons, with Cox that negligence does not suffice to prove contributory infringement; rather, at least willful blindness is required.²⁷⁴⁰

First, the court noted that Grokster’s recitation of the standard – that “[o]ne infringes contributorily by *intentionally* inducing or encouraging direct infringement” – is on its face difficult to reconcile with a negligence standard. In addition, it would have been unnecessary for the Supreme Court to discuss in detail the situations in which intent may be presumed, and those situations, like Sony, in which it may not, if liability did not require intent at all, but merely required negligence.²⁷⁴¹

Second, the Fourth Circuit analogized to patent law, in which contributory infringement requires knowledge of direct infringement, and with respect to which the Supreme Court has held that willful blindness satisfies the knowledge requirement, but recklessness and negligence do not.²⁷⁴² The Fourth Circuit was persuaded that the same rule for what qualifies as sufficient knowledge is a sensible one in the copyright context as well.²⁷⁴³ And finally, the court noted that the Second Circuit’s widely-cited Gershwin decision on contributory infringement expressly drew on the same “common law doctrine that one who *knowingly* participates or furthers a tortious act is jointly and severally liable with the prime tortfeasor.”²⁷⁴⁴

The Fourth Circuit rejected BMG’s reliance on a pre-Grokster Ninth Circuit decision, Ellison v. Robertson, in which the Ninth Circuit stated that some of its precedents had interpreted the knowledge requirement for contributory copyright infringement to include both those with actual knowledge and those who have reason to know of direct infringement.²⁷⁴⁵ The Fourth Circuit noted that the Ninth Circuit had since clarified that contributory infringement requires actual knowledge of specific acts of infringement or willful blindness of specific acts.²⁷⁴⁶

²⁷³⁹ Cox, 881 F.3d at 307-08.

²⁷⁴⁰ Id. at 308.

²⁷⁴¹ Id.

²⁷⁴² Id. (citing Global-Tech Appliances, Inc. v. SEB S.A., 563 U.S. 754, 769-71 (2011)).

²⁷⁴³ Cox, 881 F.3d at 308-09.

²⁷⁴⁴ Id. at 309 (quoting Gershwin Publ’g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)).

²⁷⁴⁵ Cox, 881 F.3d at 310 (citing Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004)).

²⁷⁴⁶ Cox, 881 F.3d at 310 (citing Luvdarts, LLC v. AT&T Mobility, LLC, 710 F.3d 1068, 1072-73 (9th Cir. 2013)).

The Fourth Circuit also rejected BMG's argument based on statements in Sony that the case at hand was one in which the defendant knew or should have known of the infringement, a situation in which the imposition of liability would be manifestly just. The Fourth Circuit noted that the Sony court's comments were referring to vicarious liability, stating that imposing liability is manifestly just where the defendant can control the use of copyrighted works by others – which is an element of vicarious liability, but not of contributory liability. Accordingly, the Fourth Circuit concluded that the district court erred in charging the jury that Cox could be found liable for contributory infringement if it knew or should have known of the infringing activity, and because there was a reasonable probability that the erroneous instruction affected the jury's verdict, the case must be remanded for a new trial.²⁷⁴⁷

The Fourth Circuit went on to address two further errors asserted by Cox in the district court's contributory infringement instructions. First, Cox contended that the district court erred in instructing the jury that Cox could be held liable for contributory copyright infringement on the basis of proof of direct infringement of BMG's copyrighted works by users of Cox's Internet services and that Cox knew of such activity. The Fourth Circuit agreed with Cox that the generalized knowledge that infringement was occurring somewhere on its network is exactly the type of knowledge that falls short under Sony. The court ruled that selling a product with both lawful and unlawful uses suggests an intent to cause infringement only if the seller knows of specific instances of infringement, but not if the seller only generally knows of infringement.²⁷⁴⁸

Put another way, the proper standard requires a defendant to have specific enough knowledge of infringement that the defendant could *do* something about it. On remand, therefore, the contributory infringement instruction should require that Cox knew of specific instances of infringement or was willfully blind to such instances.²⁷⁴⁹

Second, Cox challenged the district court's willful blindness instruction stating that Cox acted with willful blindness if it was aware of a high probability that Cox users were infringing BMG's copyrights but consciously avoided confirming that fact. The Fourth Circuit ruled that, since it had held that contributory infringement requires knowledge of, or willful blindness to, *specific instances* of infringement, the district court's willful blindness instruction should similarly require a conclusion that Cox consciously avoided learning about specific instances of

²⁷⁴⁷ Cox, 881 F.3d at 310. The court rejected BMG's argument that the jury found willful blindness when it found willful infringement by Cox. Under the willfulness instruction given by the court, the jury could find willfulness based on recklessness, a lower standard than willful blindness. Accordingly, the court could not conclude that the willfulness instruction provided a basis to hold that the jury found knowledge or willful blindness. Id. at 311 n.6.

²⁷⁴⁸ Id. at 311.

²⁷⁴⁹ Id. at 311-12 (emphasis in original).

infringement, not merely that Cox avoided confirming the fact that Cox users were infringing BMG's copyrights in general.²⁷⁵⁰

Finally, the court dispensed with Cox's challenge to the district court's willfulness instruction, arguing that it incorrectly required the jury to analyze Cox's knowledge of its *subscribers'* actions, rather than Cox's knowledge that *its actions* constituted an infringement. The court noted it had previously held that copyright infringement is willful if the defendant recklessly disregards a copyright holder's rights. Contributorily (or vicariously) infringing with knowledge that one's subscribers are infringing is consistent with at least reckless disregard for the copyright holder's rights.²⁷⁵¹

(x) Live Face on Web v. The Control Media Group

The plaintiff Live Face on Web (LFOW) owned "live person" software and a related video presentation that allowed the display of a "walking and talking" personal host who introduced a web site to an online visitor and could then be configured to explain a company's products or services and to direct the visitor's attention to a particular product or service of the web site. The defendant entered into a license agreement that allowed it to use the software and video on only one URL. The license agreement governing the software and video provided that it terminated immediately without notice from LFOW in the event the licensee failed to comply with any provision of the agreement. LFOW alleged that the defendant breached the license by using the LFOW software on two or more URLs, causing the license to terminate, and brought claims for direct, vicarious, contributory and inducement liability for the defendant's continued use of the LFOW software. The defendant brought a motion to dismiss.²⁷⁵²

The court denied the motion with respect to the claim for direct infringement, finding sufficient facts were alleged of unauthorized copying and volitional conduct necessary to plead a cause of action for direct infringement based on averments that the defendant continued to use, distribute, execute, display and cause others to unlawfully use, distribute, execute and display the LFOW software and video by loading them into the RAM of its web site visitors' and customers' computers or devices.²⁷⁵³ The court also denied the motion with respect to the claim for vicarious liability for infringement by the defendant's visitors and customers who downloaded a copy of the LFOW software into the RAM of their computers in order to view a tour of the web site. The court found it "clearly plausible" that a web site owner would, as the

²⁷⁵⁰ *Id.* at 312. The Fourth Circuit rejected Cox's argument that, with proper instructions, it was entitled to judgment as a matter of law. The court noted that at trial, BMG offered powerful evidence from which a reasonable jury could find that Cox willfully blinded itself to specific instances of infringement by its subscribers, such as evidence that Cox prevented itself from receiving any of the more than one million notices Rightscorp sent on BMG's behalf. Indeed, that appeared to be the primary theory for liability advanced by BMG. *Id.*

²⁷⁵¹ *Id.* The court also vacated the district court's grant of attorney's fee and costs to BMG and its denial of fees and costs to Cox. *Id.*

²⁷⁵² *Live Face on Web, LLC v. The Control Group Media*, 150 F. Supp. 3d 489, 493-494, 497 (E.D. Penn. 2015).

²⁷⁵³ *Id.* at 497-98.

plaintiff averred, have the right and ability to supervise the operation of its own web site. And because the LFOW software was designed to attract customers, it created a financial benefit to the defendants. Accordingly, the court ruled that LFOW had pled sufficient facts to support a claims for vicarious infringement.²⁷⁵⁴

The court, however, granted the motion with respect to LFOW's claim for contributory infringement. The defendant argued that the material contribution prong of contributory infringement cannot be premised on the mere operation of a web site business, and that the simple downloading of the LFOW software and video onto a computer's RAM was not enough for contributory infringement. The court agreed, noting that for contributory infringement, the plaintiff must allege that the defendant authorized or assisted the direct infringer, and that authorization must bear some direct relationship to the infringing acts such that the alleged contributory infringer is acting in concert with the direct infringer. The court noted that visiting a web site and downloading the LFOW software onto a computer's RAM might be the making of a copy, but it was an automated process. The court ruled that, without more, the plaintiff had not alleged sufficient facts to sustain a contributory infringement claim.²⁷⁵⁵

Finally, the court granted the motion with respect to LFOW's claim for inducing infringement. LFOW had not shown that the defendant intended visitors to infringe on the LFOW software copyright or that it had taken affirmative steps to encourage direct infringement. Accordingly, the court dismissed the inducement claim.²⁷⁵⁶

(y) BWP Media v. Polyvore

(For a discussion of contributory liability issues in this case, see Section III.C.1(g) above.)

(z) VHT v. Zillow Group

(For a discussion of contributory liability issues in this case, see Section III.C.1(i) above.)

(aa) UMG Recordings v. Grande Communications Networks

In this case, the plaintiffs brought claims of contributory and vicarious liability against Internet service provider Grande Communications Networks based on use by Grande's subscribers of peer-to-peer file sharing applications like BitTorrent to share the plaintiffs' copyrighted material without authorization. Grande moved to dismiss the plaintiffs' claims for secondary liability on the ground that the complaint failed to plead any instances of direct copyright infringement, which is a prerequisite to a claim of secondary infringement, and that

²⁷⁵⁴ *Id.* at 498-99.

²⁷⁵⁵ *Id.* at 499-500.

²⁷⁵⁶ *Id.* at 500. A case having similar facts and pleadings, in which the same plaintiff similarly survived a motion to dismiss its complaint for direct and vicarious infringement (the plaintiff did not plead contributory infringement in this case) is Live Face on Web, LLC v. KAM Development, LLC, 2016 U.S. Dist. LEXIS 175619 (N.D. Ill. Dec. 20, 2016).

providing a staple article of commerce such as Internet service cannot give rise to a claim of secondary copyright infringement. A magistrate judge recommended that the motion be granted with respect to the claim of vicarious infringement but otherwise denied.²⁷⁵⁷

With respect to direct infringement, plaintiffs pled that Grande had received notices that 1,840 of its customers had each engaged in infringement at least 100 times, based upon a software system used by Rightscorp to identify specific actual infringements of various copyrighted works by use of BitTorrent networks by Grande's users. Grande argued that the Rightscorp system was incapable of tracking or recording instances of actual copyright infringement, but instead detected only when the copyrighted material was available for distribution, which Grande asserted was insufficient to establish that direct infringement had taken place because it did not show the copyrighted material was ever requested or downloaded by a third party. Grande therefore framed the issue as a legal one – whether making a work available for copying qualifies as actual infringement. UMG, in turn, framed the issue as a primarily factual one – whether the Rightscorp system detected actual infringement, and whether the plaintiffs had adequately pled facts showing actual infringement by contending that making a copyrighted work available for copying is sufficient circumstantial evidence of actual infringement. The court noted that the parties did not dispute the basic fact that the Rightscorp system identified specific copyrighted content available for unauthorized distribution, logged that information, created a notice, and forwarded that notice to Grande.²⁷⁵⁸

The magistrate noted that the case law on the legal issue was sparse. The plaintiffs relied primarily on the district court's decision in the Cox case (discussed in Section III.C.2(w) above), in which the court found that BMG had presented sufficient circumstantial evidence of possible direct infringement based on similar information gathered by the Rightscorp system of unauthorized sharing of copyrighted material by BitTorrent users. For its part, Grande relied on a number of cases standing for the general proposition that simply making a copyrighted work available for copying is not enough to prove infringement. The magistrate observed that it could fill ten or more pages with a discussion of the subtleties of this issue, but given the stage of the proceedings, it would be a waste of time. The question before the court was whether the plaintiffs had pled enough facts to make a plausible claim that Grande's subscribers were infringing on the plaintiffs' copyrights and distributing copies of works to others through use of the BitTorrent protocol. The magistrate found that the facts pled in the complaint did so. As the trial court in the Cox case concluded, a plaintiff may rely on pleadings incorporating circumstantial evidence of copying to plead the direct infringement needed to support a claim of secondary infringement. Accordingly, the magistrate concluded that the plaintiffs' had adequately pled direct infringement.²⁷⁵⁹

²⁷⁵⁷ UMG Recordings, Inc. v. Grande Communs. Networks, LLC, 2018 U.S. Dist. LEXIS 32275 at *1-4, *6 & *33 (W.D. Tex. Feb. 28, 2018).

²⁷⁵⁸ Id. at *8-9, *12-13.

²⁷⁵⁹ Id. at *14-17.

The magistrate then turned to Grande's argument that the secondary infringement claims should be dismissed under the "staple article of commerce" doctrine of Sony because it was beyond dispute that Internet service has numerous non-infringing uses and therefore qualifies as a "staple article of commerce." The plaintiffs argued that the doctrine did not apply here because, unlike in Sony, Grande did not design a product and then place it in the stream of commerce, but instead provided a service to its subscribers, and maintained an ongoing relationship with them. The plaintiffs further argued that the Supreme Court's application of the "staple article of commerce" doctrine to copyright law is limited to arm's length transactions of a product, and was therefore inapplicable here. The magistrate noted that in the Cox case, the trial court reached the same conclusion, finding that because Cox had an ongoing relationship with its allegedly infringing subscribers, and the ability to suspend or terminate their services once they were made aware their subscribers were using the service to infringe, the staple article of commerce doctrine did not apply. The magistrate noted that other courts had reached similar results in cases involving the provision of Internet services.²⁷⁶⁰

Grande responded that it was not contending that Sony provided it a complete defense, but instead that Sony as applied and interpreted by the Supreme Court in Grokster, allows the imposition of secondary liability only when the defendant takes some sort of affirmative acts to encourage or promote subscribers to use its Internet services to infringe the plaintiffs' copyrights. Grande contended that the complaint did not allege any such affirmative acts, but rather only that Grande failed to act when the plaintiffs' made it aware its subscribers were engaged in infringement on Grande's network. The plaintiffs responded that the portion of Grokster referring to evidence of active steps taken to encourage direct infringement related only to an inducement claim, and does not apply to other theories of secondary liability, such as contributory liability. Grande countered that Sony and Grokster apply generally to all secondary copyright infringement claims, including those based upon a theory of material contribution. The magistrate noted that the most recent court to address the issue was the Fourth Circuit's decision in the Cox case, which had been issued three weeks before, in which the Fourth Circuit found that contributory liability for copyright infringement could be imposed based on willful blindness, holding that Cox's failure to act, once in receipt of the Rightscorp notices, was sufficient to show the required intent identified in Grokster. The magistrate acknowledged that this was not yet a well-defined area of the law, and there were good arguments on both sides of the issue. However, given the stage of the case, the magistrate was persuaded that the plaintiffs had pled a plausible claim of secondary infringement based on Grande's alleged failure to act when presented with evidence of ongoing, pervasive infringement by its subscribers.²⁷⁶¹

The magistrate then turned to the claim of vicarious infringement, noting that the right or ability to supervise infringement requires proof of both a legal right to stop or limit the directly infringing conduct and the practical ability to do so. The magistrate noted that Grande could stop or limit the infringing conduct by terminating its subscribers' Internet access, which was sufficient to satisfy the first element of vicarious liability. However, in order to adequately

²⁷⁶⁰ Id. at *18.

²⁷⁶¹ Id. at *19-26.

allege a direct financial benefit under the second element of vicarious liability, the plaintiffs must plead that customers subscribed to Grande's services because of the specific infringing material at issue. The magistrate noted that the closest the complaint came to addressing this requirement was an allegation that the availability of music, and particularly the plaintiffs' music, acted as a powerful draw for users of Grande's service, who used that service to download infringing music files using BitTorrent protocols. The magistrate found this insufficient to show the direct financial interest necessary to support a vicarious infringement claim. There were no allegations that Grande's actions in failing to adequately police its infringing subscribers was a draw to subscribers to purchase Grande's services, so that they could then use those services to infringe on the plaintiffs' and others' copyrights. Instead the plaintiffs alleged only that the existence of music and the BitTorrent protocol was the draw. But that logic would impose liability on every ISP, as the music at issue was available on the Internet generally, as was the BitTorrent protocol, and was not something exclusively available through Grande's services. The magistrate therefore found that the plaintiffs' vicarious copyright infringement claims should be dismissed.²⁷⁶²

The district court adopted the magistrate's recommendations for substantially the reasons stated, issuing an order dismissing the vicarious infringement claims with prejudice, but otherwise denying Grande's motion to dismiss.²⁷⁶³ Following nearly a month-long trial in Oct. 2022, a jury found Grande liable for willful contributory copyright infringement and awarded \$46.8 million in statutory damages for 1,403 of the alleged 1,422 pirated songs.²⁷⁶⁴

(bb) Cobbler Nevada v. Gonzales

This significant decision from a panel of the Ninth Circuit recapped the Ninth Circuit's approach to the two circumstances under which, following the Sony and Grokster decisions, contributory liability can be established. The court cast the issue to be decided as "whether a bare allegation that a defendant is the registered subscriber of an Internet Protocol ('IP') address associated with infringing activity is sufficient to state a claim for direct or contributory infringement. We conclude that it is not."²⁷⁶⁵

The plaintiff was the owner of a copyright in a film. It determined an IP address at which the film had been downloaded and distributed multiple times without authorization. The plaintiff was able to identify that the IP address was registered to the defendant Thomas

²⁷⁶² Id. at *26-29.

²⁷⁶³ Order on Report and Recommendation of the United States Magistrate Judge, UMG Recordings, Inc. v. Grande Communs. Networks LLC, Case 1:17-cv-00365-LY (W.D. Tex. Mar. 26, 2018).

²⁷⁶⁴ "ISP Owes Record Cos. \$47M Over Song Piracy, Jury Says," *Law360* (Nov. 3, 2022), available as of Nov. 3, 2022 at <https://www.law360.com/articles/1546618/isp-owes-record-cos-47m-over-song-piracy-jury-says>. The judge denied a subsequent motion by Grande Communications for judgement in its favor as a matter of law or a new trial. "ISP Loses Bid for Retrial after \$47M Copyright Verdict," *Law 360* (May 11, 2023), available as of May 14, 2023 at <https://www.law360.com/articles/1607072/>.

²⁷⁶⁵ Cobbler Nev., LLC v. Gonzales, 901 F.3d 1142, 1144 (9th Cir. 2018).

Gonzales, who operated an adult foster care home, and amended its complaint to name Gonzales as the sole defendant, asserting claims of direct and contributory liability. The Ninth Circuit first stated that the direct infringement claim failed because Gonzales's status as the registered subscriber of an infringing IP address, standing alone, did not create a reasonable inference that he was also the infringer because multiple devices and individuals may be able to connect via an IP address. A plaintiff must therefore allege something more to create a reasonable inference that a subscriber was also an infringer.²⁷⁶⁶

The court then turned to the contributory infringement claim. The plaintiff based its contributory claim on the theory that Gonzales facilitated and promoted the use of the Internet for infringing the plaintiff's copyright rights by failing to reasonably secure, police and protect the use of his Internet service. The plaintiff alleged that Gonzales had been sent over 400 notices of infringing activity, yet failed and refused to take any action whatsoever and continued to allow infringing activity after such notices.²⁷⁶⁷

The court began its contributory analysis by quoting the "well-settled rule" that "[o]ne infringes contributorily by intentionally inducing or encouraging direct infringement."²⁷⁶⁸ A claim for contributory infringement requires allegations that the defendant is "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another."²⁷⁶⁹ The court noted that the plaintiff's contributory infringement claim was premised on a bare allegation that Gonzales failed to police his Internet service, and that such perfunctory allegation, without more, did not sufficiently link Gonzales to the alleged infringement. Although noting that Gonzales's position – a subscriber to Internet service – did not fit cleanly within the Ninth Circuit's typical contributory liability framework, which often involves consumer-facing Internet platforms, nevertheless the court found it to be no leap to apply the framework of similar technology-based cases to its analysis of Gonzales's liability.²⁷⁷⁰

The court then turned to the analysis of contributory liability set forth in the Supreme Court's Sony and Grokster cases. The Ninth Circuit observed that the Grokster court noted that the limitation of liability in Sony – premised on a refusal to impute intent to a defendant based solely on knowledge that a product might be used for infringement – did not apply where evidence shows statements or actions directed to promoting infringement. The Ninth Circuit further observed that the Grokster court was clear, however, that in the absence of other evidence of intent, a court would be unable to find contributory infringement liability merely

²⁷⁶⁶ Id. at 1145-47.

²⁷⁶⁷ Id. at 1145-46.

²⁷⁶⁸ Id. at 1147 (citing Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1170 (9th Cir. 2007) (quoting Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005))).

²⁷⁶⁹ Cobbler, 901 F.3d at 1147 (quoting Fonovisa v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996)).

²⁷⁷⁰ Cobbler, 901 F.3d at 1147-48.

based on a failure to take affirmative steps to prevent infringement, if the device otherwise was capable of substantial noninfringing uses.²⁷⁷¹

In a quite significant ruling, the Ninth Circuit then stated: “Although circuit courts approach contributory liability through varying lenses, our circuit has identified two strands of liability following Sony and Grokster: [i] ‘actively encouraging (or inducing) infringement through specific acts’ or [ii] ‘distributing a product distributees use to infringe copyrights, if the product is not capable of “substantial” or “commercially significant” noninfringing uses.’ Amazon, 508 F.3d at 1170 (quoting Grokster, 545 U.S. at 942 (Ginsburg, J., concurring)).”²⁷⁷² This formulation of the standard for contributory liability is narrower than the formulations by the Ninth Circuit in other cases, such as the Perfect 10 v. Visa case that came before Cobbler Nevada and the Kast case that came after it (discussed in the next subsection).

Turning to the first strand, the Ninth Circuit noted that the plaintiff’s complaint lacked any allegations that Gonzales actively encouraged or induced infringement through specific acts. Nothing in the complaint alleged, or even suggested, that Gonzales actively induced or materially contributed to the infringement through purposeful, culpable expression and conduct. Nor did any allegations suggest Gonzales made any clear expression or took affirmative steps to foster the infringement – Gonzales’s only alleged action was his failure to secure, police and protect the connection. Nor did the second strand implicate Gonzales. The court observed that providing Internet access could hardly be said to be distributing a product or service that was not capable of substantial or commercially significant noninfringing uses. The court noted that the plaintiff’s theory both strayed from precedent and effectively created an affirmative duty for private Internet subscribers to actively monitor their Internet service for infringement. Imposing such a duty would put at risk any purchaser of Internet service who shared access with a family

²⁷⁷¹ Id. at 1148.

²⁷⁷² Id. A district court within the Sixth Circuit, noting that no decisions on contributory infringement had been issued by the Sixth Circuit since the Supreme Court’s Grokster decision, adopted the Cobbler court’s formulation of contributory infringement based on Justice Ginsburg’s concurrence in Grokster:

“In Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., the Supreme Court reformulated the standard for imposing liability for contributory copyright infringement, stating succinctly that ‘one infringes contributorily by intentionally inducing or encouraging direct infringement.’ Id. 545 U.S. 913, 930 (2005). Within that general standard, the Court identified two categories of liability, which Justice Ginsburg summarized as follows: ‘Liability under our jurisprudence may be predicated on actively encouraging (or inducing) infringement through specific acts (as the Court’s opinion develops) or distributing a product distributees use to infringe copyrights if the product is not capable of ‘substantial’ or ‘commercially significant’ noninfringing uses.’ Grokster, 545 U.S. at 36-37, 942 (Ginsburg, J., concurring). Under Grokster, a plaintiff must show that the defendant (1) provides a product or service incapable of substantial noninfringing use or (2) intentionally induces infringement by clear expression or other affirmative steps to foster infringement.”

“Other circuit courts have found that contributory infringement requires wrongful intent with ‘purposeful, culpable expression and conduct.’ Cobbler Nevada, LLC v. Gonzales, No. 17-35041, 2018 WL 4055766 at *4 (9th Cir., Aug. 27 2018) (quoting Grokster, 545 U.S. at 937). A mere failure to act, such as a failure to police an Internet service or a failure to take affirmative steps to prevent infringement, does not suffice for contributory infringement. Id. at *4 (quoting Grokster, 545 U.S. at 939 n.12). Nor does mere knowledge of actual infringing uses of a service suffice. Id. (quoting Grokster, 545 U.S. at 937).” Average Joe’s Entm’t Group v. Soundcloud, Ltd., 2018 U.S. Dist. LEXIS 225151 at *7-8 (M.D. Tenn. Oct. 17, 2018).

member or roommate, or who was not technologically savvy enough to secure the connection to block access by a frugal neighbor. The court concluded that the facts of this case hardly seemed to be one of the circumstances in which it would be just to hold one individual accountable for the actions of another. The court therefore affirmed the district court's dismissal of the plaintiff's claims.²⁷⁷³

(cc)Erickson Prods. v. Kast

The defendant Kast, owner of a real estate wealth management company, hired a company called Only Websites to redevelop his web site. Kast identified Wells Fargo Private Bank as one of his competitors and highlighted certain features of Wells Fargo's web site he found appealing. Three photos from Wells Fargo's web site, which were taken by the plaintiff, were incorporated into Kast's web site without a license. The plaintiff demanded that Kast stop infringing his copyright and pay damages. Kast promptly directed Only Websites to remove the photos, which was done the next morning, but refused to pay. The plaintiff filed suit alleging direct, vicarious and contributory copyright infringement and that the infringement was willful. A jury found that Kast vicariously and contributorily infringed the plaintiff's copyrights on the photos and awarded a total of \$450,000 in damages. Kast appealed, initially briefing his case without the assistance of counsel. The Ninth Circuit appointed pro bono counsel to assist Kast with two of the issues raised in his opening brief: (1) whether the avoidance of licensing fees constitutes a direct financial benefit for purposes of imposing vicarious copyright liability, and (2) whether a "should have known" willfulness instruction is proper under Section 504(c).²⁷⁷⁴

Turning first to the vicarious liability verdict, the court focused on the direct financial benefit requirement, noting that a web site owner can receive a direct financial benefit from the presence of infringing material on the site only where the availability of infringing material acts as a draw for customers, rather than just an added benefit. Here the court noted that, although the plaintiff claimed the photos enhanced the general attractiveness of Kast's web site to customers and thereby drew visitors to purchase his services, he did not contend that anyone visited the site in order to view his photos or purchased services from Kast because they saw the photos. Thus, the plaintiff had not shown that the photos were anything more, at best, than an added benefit to visitors of the site.²⁷⁷⁵

Alternatively, the plaintiff asserted that Kast enjoyed a direct financial benefit from the illegal copying by avoiding the license fees he would otherwise have been required to pay. The court noted that whether a vicarious infringer's avoidance of licensing fees constitutes a direct financial benefit as a matter of law was a question of first impression in the Ninth Circuit, and no other Circuit had addressed it either. The court held that it does not. The court observed that, as an initial matter, the avoidance of fees claim could not be premised on any unlicensed use by

²⁷⁷³ Cobbler, 901 F.3d at 1144, 1148-49. The court also determined that the district court did not abuse its discretion by awarding Gonzales attorneys' fees. Id. at 1149-50.

²⁷⁷⁴ Erickson Prods. v. Kast, 921 F.3d 822, 826-28 (9th Cir. 2019).

²⁷⁷⁵ Id. at 829-30.

Kast of the plaintiff's photos, because that would result in direct liability, a theory the jury rejected. Instead, the plaintiff's argument must be that Kast received a direct financial benefit when Only Websites, the direct infringer, avoided the plaintiff's licensing fee. The court ruled that the direct infringer's avoidance of fees alone cannot satisfy the requirement of a direct financial benefit to the vicarious infringer. Otherwise, the requirement of a direct financial benefit would be rendered meaningless since – at least where, as here, licenses were for sale – a direct infringer necessarily saves money by failing to obtain a license. Nor had Kast received any other direct financial benefit as result of Only Websites' failure to pay. In some circumstances, a direct infringer's avoidance of fees might prove financially advantageous to a vicarious infringer – here, for example, Kast could have benefitted if Only Websites turned its lower costs from fee avoidance into lower prices for its web site design services. But the plaintiff never claimed that Only Websites and Kast were able to offer services more cheaply or quickly because Only Websites infringed Erickson's copyright.²⁷⁷⁶

The court rejected the plaintiff's further argument that Kast received a direct financial benefit because the photos enabled Kast to rush the launch of his web site. The court noted that, although Kast had rushed the site out before it was finished in order to seek appointment to manage certain estates, Kast received no money, clients, business inquiries, or web site visitors by rushing the web site's completion before removing the plaintiff's photos.²⁷⁷⁷

Turning to the contributory liability verdict, the court stated that a party engages in contributory copyright infringement when it (1) has knowledge of another's infringement and (2) either (a) materially contributes to or (b) induces that infringement, citing its Perfect 10 v. Visa decision. Note that this formulation of the contributory liability standard is different from the narrower formulation of that standard articulated by the Ninth Circuit panel in the 2018 Cobbler Nevada decision (discussed in the previous subsection). Kast asserted that the trial judge erred by instructing the jury that "knowledge" for contributory infringement purposes includes having "reason to know" of the infringement. Kast asserted that only actual knowledge or willful blindness are sufficient. The court responded that, because Kast did not raise objection to the jury instruction at trial, it would be reviewed on appeal only for plain error. The court ruled that, even if the "should have known" instruction was erroneous, the error was not plain **given acknowledged inconsistency in Ninth Circuit case law on the "knowledge" element of contributory liability**. For instance, in its Luvdarts v. AT&T Mobility case (discussed in Section III.C.3(o)), the Ninth Circuit held that actual knowledge of specific acts of infringement and willful blindness of specific acts are the only two mental states that satisfy the knowledge element of contributory infringement. But in Louis Vuitton v. Akanoc (discussed in Sections III.C.1(a) and III.C.2(j)), the Ninth Circuit cited with approval a "know or have reason to know" instruction for contributory liability. While Luvdarts was decided after Louis Vuitton, it did not expressly

²⁷⁷⁶ Id. at 830-31. The court also rejected the plaintiff's argument that Only Websites avoided the licensing fee in its capacity as Kast's agent, such that Kast himself should be liable for its failure to pay. Only Websites' decision to infringe the plaintiff's copyright would have exceeded the scope of any agency relationship that may have existed between them. Id. at 831.

²⁷⁷⁷ Id.

overrule it. And both cases were decided several years after the Supreme Court's Grokster decision, the case in which Kast claimed the Supreme Court settled the matter in favor of an "actual knowledge" requirement. So the panel in this case elected not to attempt to resolve the apparent tension between Luvdarts and Louis Vuitton, and instead simply held that Kast had not demonstrated the jury instructions were plainly erroneous.²⁷⁷⁸

Finally, the court turned to Kast's claim with respect to the willfulness finding that the district court erred when it instructed the jury that it could find Kast's infringement was willful if Kast should have known that his acts infringed the plaintiffs' copyright. The court agreed, citing previous Ninth Circuit authority that to prove willfulness, the plaintiff must show (1) that the defendant was actually aware of the infringing activity or (2) that the defendant's actions were the result of reckless disregard for, or willful blindness to, the copyright holder's rights. The court noted that a "should have known" instruction does not fit within this framework because it is a negligence standard. Negligence is a less culpable mental state than actual knowledge, willful blindness, or recklessness – the three mental states that properly support a finding of willfulness. The court found that the erroneous willfulness instruction given by the district court was likely prejudicial to Kast, rejecting the plaintiff's contention that, if Kast had "knowledge" for purposes of contributory infringement, he had "knowledge" for purposes of the willfulness inquiry. Under some of the Ninth Circuit's inconsistent formulations of the knowledge requirement for contributory infringement, "reason to know" can be sufficient knowledge, and "reason to know" is a negligence standard that is inconsistent with the higher standard of knowledge required for willfulness.²⁷⁷⁹ The court therefore concluded, "We have never held merely negligent conduct to be willful, and we decline to do so now."²⁷⁸⁰

In sum, the court vacated the jury's finding of vicarious liability, affirmed the jury's finding of contributory liability (and therefore affirmed the judgment), reversed the jury's finding of willfulness, and remanded the issue of willfulness to the district court.²⁷⁸¹

(dd) Oppenheimer v. Morgan

The plaintiff brought copyright infringement claims alleging publication of two of his copyrighted photos on a web site owned by the defendant Capital at Play, Inc. The plaintiff also asserted copyright claims, including contributory infringement claims, against individual defendant Harley Morgan, a principal of Capital at Play who controlled nearly all decisions of the company. The court dismissed the contributory infringement claim against Morgan.²⁷⁸²

²⁷⁷⁸ Id. at 831-32.

²⁷⁷⁹ Id. at 833-345.

²⁷⁸⁰ Id. at 834.

²⁷⁸¹ Id. at 836.

²⁷⁸² Oppenheimer v. Morgan, 2019 U.S. Dist. LEXIS 106944 at *1-4 (W.D.N.C. June 26, 2019).

The court cited the Supreme Court's statement in Grokster that "One infringes contributorily by intentionally inducing or encouraging direct infringement"²⁷⁸³ and the Fourth Circuit's statement in BMG v. Cox Communications that "Proving contributory infringement requires proof of at least willful blindness; negligence is insufficient."²⁷⁸⁴ The plaintiff alleged that Morgan caused, enabled, facilitated, and/or materially contributed to the infringements. However, the plaintiff made no allegation that Morgan induced or encouraged another to infringe the plaintiff's copyrights, but rather alleged only that Morgan was the decision maker for the defendant Capital at Play. The court therefore ruled that, although the plaintiff's allegations were sufficient for a claim of direct infringement against Morgan, they were inconsistent with a claim for contributory infringement. Accordingly, the court dismissed the contributory liability claim against Morgan.²⁷⁸⁵

(ee) King v. Amazon

In this case the plaintiff, Ernest King, brought a copyright infringement claim against Amazon for publication of his book, *From Brooklyn to the Grave*, through Amazon's self-publishing service known as CreateSpace. The plaintiff authored the book while incarcerated, obtaining the help of Regina Thomas, his former girlfriend, in the editing process and to assist him in finding a publisher. King brought a pro se complaint that was confusingly worded, but which the court liberally construed to assert, among other causes of action, one for direct and indirect copyright infringement. Amazon filed a motion for summary judgment, to which King did not respond timely. The court found that Amazon correctly asserted King could not show that any distribution through Amazon was unauthorized because he admitted that Thomas was assisting him in editing and finding a publisher, her name was listed as the person to contact for rights and permissions on the Certificate of Registration King submitted as an exhibit and as the copyright owner for the book on the Copyright Office's Online Public Catalog. The court therefore found no dispute of fact that Thomas was at all times working as King's authorized agent in getting the book published through CreateSpace.²⁷⁸⁶

Turning to the issue of secondary infringement, Amazon argued that King could not show secondary infringement because King could not establish direct infringement by any party. Because Amazon brought its motion for summary judgment, the court did not decide whether Thomas infringed King's copyright because the court concluded that King in any event could not show that Amazon contributorily or vicariously infringed on his copyright even if Thomas was a direct infringer.²⁷⁸⁷ The court stated that to establish contributory infringement, "a plaintiff must show that the defendant (1) provides a product or service incapable of substantial non-

²⁷⁸³ Id. at *7 (citing Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005)).

²⁷⁸⁴ 2019 U.S. Dist. LEXIS 106944 at *8 (citing BMG Rights Mgmt. (US) LLC v. Cox Commc'ns, Inc., 881 F.3d 293, 310 (4th Cir. 2018)).

²⁷⁸⁵ 2019 U.S. Dist. LEXIS 106944 at *8.

²⁷⁸⁶ King v. Amazon Corp., 2019 U.S. Dist. LEXIS 205763 at *1-2, *1-8 (W.D.N.C. Nov. 27, 2019).

²⁷⁸⁷ Id. at *11.

infringing uses, or (2) intentionally induces infringement by clear expression or other affirmative steps to foster infringement.”²⁷⁸⁸ The court concluded that King could not show that CreateSpace was incapable of a substantial non-infringing use because millions of non-infringing self-published books were published through it. The court also concluded that King could not show that Amazon intentionally induced or encouraged direct infringement of his copyright because Amazon played a purely passive role in the publication of King’s book. Accordingly, the court granted Amazon summary judgment on any contributory infringement claim.²⁷⁸⁹

(ff) Sony Music v. Cox Communications

This case involved very similar claims of contributory infringement as those brought in the BMG v. Cox Communications case, discussed in Section III.C.2(w) above. Several record companies, owners of copyrights in multiple sound recordings and musical compositions, brought claims for indirect copyright infringement against Cox Communications based on sharing of infringing music files by its cable subscribers using peer-to-peer (P2P) networks. The RIAA, acting as the plaintiffs’ agent, hired an anti-piracy company, MarkMonitor, to scan the Internet for potentially infringing file sharing on P2P networks. MarkMonitor acted as a participant in the P2P networks to engage with potentially infringing users, gather data from those users, and use that data to generate infringement notices, which it sent to Cox to be delivered to the Cox subscribers holding Cox Internet service accounts at the IP addresses identified by MarkMonitor where infringing sharing was taking place. Through MarkMonitor, the plaintiffs identified individual Cox accounts that received three or more infringement notices and used those subscribers as the basis for their secondary infringement claims against Cox. The plaintiffs claimed that Cox was liable for infringement of 7,068 copyrighted sound recordings and 3,452 copyrighted musical compositions from Feb. 1, 2013 until Nov. 26, 2014.²⁷⁹⁰

The plaintiffs moved for partial summary judgment that Cox had knowledge of infringement for purposes of contributory infringement. The court summarized a claim for contributory infringement in its classic formulation: “[o]ne contributorily infringes when he (1) has knowledge of another’s infringement and (2) either (a) materially contributes to or (b) induces that infringement.”²⁷⁹¹ The court further noted that, under the Fourth Circuit’s decision in the BMG v. Cox Communications case, contributory liability can be based on willful blindness but not on recklessness or negligence. The Fourth Circuit also ruled that generalized knowledge of infringement somewhere on an OSP’s network is insufficient to establish contributory

²⁷⁸⁸ Id. (citing Average Joe’s Entm’t Grp., LLC v. SoundCloud, LTD., 2018 U.S. Dist. LEXIS 225151 at *4 (M.D. Tenn. Oct. 17, 2018) (citing MGM Studios v. Grokster, Ltd., 545 U.S. 913, 936-37 & 942 (2005))).

²⁷⁸⁹ Id. at *12-14. The court also concluded that King could not prevail on a vicarious infringement claim because he could not show that Amazon had the practical ability to supervise the millions of authors and independent publishers who utilized its self-publishing services. Id. at * 15-16.

²⁷⁹⁰ Sony Music Entm’t v. Cox Communs., Inc., 426 F. Supp. 3d 217, 221 (E.D. Va. 2019).

²⁷⁹¹ Id. at 230 (quoting Perfect 10, Inc. v. Visa Int’l Serv. Ass’n, 494 F.3d 788, 795 (9th Cir. 2007)).

infringement liability – the proper standard requires a defendant to have specific enough knowledge of infringement that the defendant can do something about it.²⁷⁹²

Here, MarkMonitor’s notices included the timestamp of the infringement detection, the date the notice was sent to Cox on behalf of the RIAA, the Cox user (identified by IP address and Port), a hash value pertaining to the file, and all additional data required by Section 512(c)(3) of the DMCA. The notices also informed subscribers that if they disagreed with the claims in the notice, they should contact the sender, and not Cox, to resolve the matter. The court ruled that based on the level of detail included in the notices, there was no doubt that Cox had more than just generalized knowledge of infringement on its network, and because Cox maintained the ability to suspend or terminate the infringing accounts, it had specific enough knowledge of infringement that it could *do* something about it.²⁷⁹³

Cox argued that because each notice specified only one particular work (Artist/Title pair), the opaque reference to an info hash in the notice did not on its face disclose that other works might have been on the subscriber’s computer. The court found this argument misplaced, because the governing law is focused on the infringing conduct, not the specifics of the content of the notice. The Fourth Circuit established a floor for a prima facie showing of knowledge and the MarkMonitor notices lay well above that floor, given the complex and detailed information they contained.²⁷⁹⁴ The court concluded, “However you define this floor, the DMCA safe harbor does not apply in this litigation, and Plaintiffs should not be held to provisions that are more demanding than the underlying applicable law.”²⁷⁹⁵ The court therefore found as a matter of law that there was no genuine issue of fact regarding the sufficiency of the notices in the case, and that they could support the knowledge element of a contributory infringement claim.²⁷⁹⁶

The plaintiffs’ motion went further, however, seeking a ruling that the notices were not only able to support the knowledge element, but also dispositive of knowledge on these facts. The court agreed, noting that the notices both documented a specific instance of infringement and notified Cox of that instance. After receiving a notice, Cox could have acted in several capacities – for instance, it could have further evaluated the subscriber’s overall activity or terminated that subscriber. In sum, the court found the plaintiffs had established the knowledge element of contributory liability by showing knowledge of specific conduct which allegedly infringed all sound recordings and musical compositions identified in suit. No genuine issue material facts remained.²⁷⁹⁷

²⁷⁹² Sony Music v. Cox, 426 F. Supp. 3d at 230 (citing BMG Rights Mgmt. (US) LLC v. Cox Communs, Inc., 881 F.3d 293, 309, 311 (4th Cir. 2018)).

²⁷⁹³ Sony Music v. Cox, 426 F. Supp. 3d at 231-32.

²⁷⁹⁴ Id. at 232.

²⁷⁹⁵ Id.

²⁷⁹⁶ Id.

²⁷⁹⁷ Id. at 232-33.

Cox asked the court to find as a matter of law that Cox could not be liable for potential infringement by any end users of Cox Business accounts because the notices identified alleged infringers only by the IP address of the Cox Business subscriber and the IP address alone did not identify which user of a particular Cox Business subscriber's IP address was the purported infringer. Cox relied on the Ninth Circuit's decision in the Cobbler case, discussed in Section III.C.2(bb) above. The court rejected this argument, noting that an important distinction in Cobbler was that the fundamental conundrum in that case was finding and naming the right defendant, since the individual who owned the Internet account had not undertaken any of the allegedly infringing activity. The court noted that in this case, there was no dispute or hesitation in naming Cox as the intended defendant. In addition, the fact that Cox was an OSP was material, because the law recognizes and treats service providers differently from end users, and Cobbler's holdings and dicta are relevant to individual account holders, not the provider of the account.²⁷⁹⁸

The court elaborated that the reason there was no doubt as to the intended defendant in this case is because the case involved "a large-scale attempt to impose indirect liability where enforcement against direct infringers is both impractical and improbable."²⁷⁹⁹ The court noted the natural analogy is that Cox had the information to identify its subscribers in this case, just as Comcast had the information to identify its individual subscriber in Cobbler. Cox had the access and ability to use individual account information associated with the IP addresses at issue, not the plaintiffs. Yet Cox had not produced evidence of any organized endeavor to identify direct infringers beyond the Cox Business IP addresses.²⁸⁰⁰ "Ultimately, the characterization of an IP address as a residence or a business does not affect either the level of specificity in the notice or Cox's ability to take action in response. There is no indication from the Fourth Circuit that specific IP addresses and account numbers are insufficient to identify 'particular subscribers,' and consequently, the knowledge standard discussed herein applies to all subscribers that were the subject of a notice from Plaintiffs."²⁸⁰¹ The court therefore ruled that neither the Fourth Circuit's BMG decision nor the Cobbler decision precluded a jury from finding that Cox had actual knowledge of or was willfully blind to infringement by residential and business subscribers alike. The court granted the plaintiffs summary judgment as to knowledge of specific instances of copyright infringement, both as to individual and business subscribers.²⁸⁰²

(gg) ALS Scan v. Steadfast Networks

In this case (designated as not appropriate for publication and not precedent except as provided by Ninth Circuit Rule 36-3), the Ninth Circuit affirmed a grant of summary judgment in favor of the defendant, a data-center service provider, on the plaintiff's claim for contributory

²⁷⁹⁸ Id. at 233-35.

²⁷⁹⁹ Id. at 235.

²⁸⁰⁰ Id. at 235-36.

²⁸⁰¹ Id. at 236.

²⁸⁰² Id.

infringement. The defendant's data center hosted a web site, Imagebam.com, on which users uploaded content. That web site had allegedly become an unauthorized hub of copyrighted adult material, some of which was created by the plaintiff. The plaintiff sent multiple notices of copyright infringement to the defendant about the images on Imagebam. Whenever it received a notice, the defendant forwarded it to the designated agent for Imagebam. Every copyrighted image at issue was then removed by Imagebam.²⁸⁰³

The court affirmed that the defendant was not liable for contributory infringement because it had taken "simple measures" to prevent further damage to the plaintiff's copyrighted works. The plaintiff asserted that the defendant's corporate representative testified during his deposition that the defendant did nothing to follow up with the owner of Imagebam after forwarding the notices. The court ruled that whether or not the defendant followed up was irrelevant because it was undisputed that the defendant forwarded the notices and the infringed images were taken down. The plaintiff asserted that it was not enough to forward the infringement notices to Imagebam's owner in view of the number of infringement notices that the defendant had received. But the court ruled that the number of notices was legally irrelevant because the knowledge required for contributory liability is more than a generalized knowledge of the possibility of infringement – actual knowledge of specific acts of infringement is required. The number of notices received gives at most a general knowledge that infringement will likely occur again in the future but does not give notice of any specific acts of infringement that are actually occurring. The defendant forwarded every notice it received of actual infringement to Imagebam's owners, and every infringing work was taken down. There was no evidence that the defendant had any other simple measures at its disposal. The defendant did not operate, control, or manage any functions of Imagebam.com. And it could not supervise, access, locate, or delete Imagebam accounts. It had no way of knowing, based on a URL hyperlink contained in the notices of copyright infringement, where the infringing works or the Imagebam accounts responsible for illegal uploads were located on its servers. Accordingly, the court ruled that the defendant took what measures were available to it to prevent further damage to the plaintiff's copyrighted images.²⁸⁰⁴

(hh) Atari v. Redbubble

(For a discussion of contributory liability issues in this case, see Section III.C.1(j) above.)

²⁸⁰³ ALS Scan, Inc. v. Steadfast Networks, LLC, 2020 U.S. App. LEXIS 22360 at *2-3 (9th Cir. July 17, 2020).

²⁸⁰⁴ Id. at *3-6. A dissenting judge argued that the majority incorrectly interpreted the standard of contributory infringement to require that an operator can be held liable only if it continues to provide access to the very same infringing works. But the standard used in previous Ninth Circuit cases looks to whether the operator continued to provide access to "infringing works," including other infringing works. The dissenting judge observed that a focus on future infringement is also consistent with the DMCA safe harbors, which shield only those service providers who have adopted and reasonably implemented a repeat infringer policy. Id. at *7-10.

(ii) Mon Cheri Bridals v. Cloudflare

The plaintiffs sold wedding dresses online, but their sales numbers and brand reputations were damaged by the proliferation of counterfeit retailers that sold knock-off dresses using the plaintiffs' copyrighted images. The plaintiffs had gone after the infringers in a range of actions, but to no avail – every time a website was successfully shut down, a new one took its place. In an effort to more effectively stamp out infringement, the plaintiffs sought to hold Cloudflare contributorily liable for the infringement on the ground that it provided the infringers with caching, faster content delivery, and security services. The court granted summary judgment to Cloudflare, holding that simply providing services to a copyright infringer does not qualify as a material contribution to the infringement. Rather, liability in the Internet context follows where a party facilitates access to infringing websites in such a way that significantly magnifies the underlying infringement.²⁸⁰⁵

The plaintiffs had not offered any evidence that faster load times would be likely to lead to significantly more infringement than would occur without Cloudflare. Nor did Cloudflare's security services materially contribute to infringement. From the perspective of a user accessing the infringing websites, those services made no difference. The court observed that if Cloudflare's provision of those services made it more difficult for a third party to report incidents of infringement to the web host as part of an effort to get the underlying content taken down, perhaps it could be liable for contributory infringement. But here, the parties agreed that Cloudflare informed complainants of the identity of the host in response to receiving a copyright complaint, in addition to forwarding the complaint along to the host provider.²⁸⁰⁶

(jj) Some Observations

An OSP, BBS operator or other operator of an online service can be liable for contributory infringement where the operator has sufficient knowledge of infringing activity. The level of knowledge required is not consistent among the cases and is confusingly explicated in some of them, including the Ninth Circuit's rulings in the Napster cases. The Ellison and Perfect 10 v. Cybernet Ventures cases seem to hold that constructive knowledge, or reason to know of infringement, may be sufficient for contributory liability. However, the Ninth Circuit's Napster cases seemed to adopt a standard of "reasonable knowledge," as Judge Patel's extensive analysis of those cases concludes in her opinion in the Hummer Winblad case, discussed in Section III.C.2(c)(7) above. As Judge Patel concluded, the precise scope of this standard of "reasonable knowledge" is not clear, but it seems to be narrower than the "reason to know" standard of constructive knowledge used in the Ellison and Perfect 10 v. Cybernet Ventures cases.

To add to the confusion, under the Ninth Circuit's Grokster decision, where contributory liability is alleged based on the distribution of a product or service used to infringe, the level of

²⁸⁰⁵ Mon Cheri Bridals, LLC v. Cloudflare, Inc., 2021 U.S. Dist. LEXIS 193199 at *1-2 (N.D. Cal. Oct. 6, 2021) (citing Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1172 (9th Cir. 2007)).

²⁸⁰⁶ Id. at *

knowledge required for contributory liability varies with whether the product or service of the defendant has substantial noninfringing uses. If the product at issue is not capable of substantial or commercially significant noninfringing uses, then the copyright owner need only show that the defendant had constructive knowledge of the infringement. On the other hand, if the product at issue is capable of substantial or commercially significant noninfringing uses, then the copyright owner must demonstrate that the defendant had reasonable knowledge of specific infringing files and failed to act on that knowledge to prevent infringement. The Ninth Circuit's Grokster decision interpreted the Napster I decision as requiring actual knowledge of specific infringing acts at a time during which the OSP materially contributes to the infringement in order for there to be contributory liability for such acts. However, the Supreme Court's Grokster decision found that the Ninth Circuit erred in the latter ruling, so it is unclear how much of the Ninth Circuit's adjudication of the knowledge requirement for contributory liability survive the Supreme Court's Grokster ruling. In her analysis of this issue in her opinion in the Hummer Winblad case, Judge Patel was able to conclude only that the Supreme Court's rejection of the Ninth Circuit's ruling suggests that, taken as a whole, the Supreme Court's decision provided for liability under broader circumstances than those permitted under Napster I, but the precise scope of that liability remained unclear.

More recently, the Erickson Prods. v. Kast case candidly acknowledged inconsistency in Ninth Circuit case law on the "knowledge" element of contributory liability. For instance, the Kast court noted that in Luvdarts v. AT&T Mobility case (discussed in Section III.C.3(o)), the Ninth Circuit held that actual knowledge of specific acts of infringement and willful blindness of specific acts are the only two mental states that satisfy the knowledge element of contributory infringement. But in Louis Vuitton v. Akanoc (discussed in Sections III.C.1(a) and III.C.2(j)), the Ninth Circuit cited with approval a "know or have reason to know" instruction for contributory liability. While Luvdarts was decided after Louis Vuitton, it did not expressly overrule it. And both cases were decided several years after the Supreme Court's Grokster decision, the case in which Kast claimed the Supreme Court settled the matter in favor of an "actual knowledge" requirement. So the panel in the Kast case elected not to attempt to resolve the apparent tension between Luvdarts and Louis Vuitton, and instead simply disposed of the case by ruling that Kast had not demonstrated the jury instructions were plainly erroneous.

Beyond knowledge, how much the operator must contribute to the infringing activity after gaining such knowledge beyond the mere provision of the facilities used to accomplish the infringement is also unclear. The Ninth Circuit's interpretation in the Napster I case of its Fonovisa decision seems to require little more than continuing to provide such facilities after knowledge that infringing activity is taking place. The MAPHIA, CoStar and Ellison courts interpreted the Netcom decision to require more (note that, although the Netcom case was decided before both Fonovisa and Napster I, the CoStar and Ellison cases were decided after Fonovisa and Napster I). And other later decisions discussed above have required more.

As discussed in detail above, the Ninth Circuit's Napster I decision contains a number of ambiguities with respect to the scope of the duty to police for occurrences of infringing material upon receipt of knowledge. However, the cases seem to require at least that a service provider

actively attempt to verify a claim of infringement after receiving notice of the same and to take appropriate action in response. In addition, several decisions have imposed contributory liability on the part of a BBS where the BBS operator actively encouraged the acts leading to the infringements. See the discussions of the Sabella case²⁸⁰⁷ and the Hardenburgh case²⁸⁰⁸ above, although these cases were not all based expressly on an inducement theory of contributory liability.

More generally, there is not uniformity among the courts as to the standard for contributory infringement applicable to an OSP after the Supreme Court’s Grokster decision – and particularly whether the Grokster decision limited contributory infringement to inducement, or whether both an inducement and a “material contribution” theory of contributory liability survive. This lack of uniformity is well illustrated within the Ninth Circuit. For example, in its 2019 decision in Erickson Prods. v. Kast (discussed in Section II.C.2(cc) above), the Ninth Circuit stated that a party engages in contributory copyright infringement when it (1) has knowledge of another’s infringement and (2) either (a) materially contributes to or (b) induces that infringement, citing its 2007 Perfect 10 v. Visa decision. This formulation of the contributory liability standard is different from a narrower formulation of that standard articulated earlier by a Ninth Circuit panel in its 2018 Cobbler Nevada decision (discussed in Section II.C.2(bb) above), in which it stated: “Although circuit courts approach contributory liability through varying lenses, our circuit has identified two strands of liability following Sony and Grokster: [i] ‘actively encouraging (or inducing) infringement through specific acts’ or [ii] ‘distributing a product distributees use to infringe copyrights, if the product is not capable of “substantial” or “commercially significant” noninfringing uses.’ Amazon, 508 F.3d at 1170 (quoting Grokster, 545 U.S. at 942 (Ginsburg, J., concurring)).”

Some cases decided after these Ninth Circuit cases have applied the narrower formulation of contributory liability that focuses on inducement or distribution of a product that is not capable of substantial noninfringing uses:

- Oppenheimer v. Morgan (W.D.N.C. 2019), discussed in Section II.C.2(dd) above
- King v. Amazon (W.D.N.C. 2019), discussed in Section II.C.2(ee) above

However, other cases decided after these Ninth Circuit decisions continue to apply the more classic formulation of the contributory liability test:

- Sony Music v. Cox Communications (E.D. Va. 2019), discussed in Section II.C.2(ff) above)

As discussed in Section III.C.6(b) below, the DMCA defines certain safe harbors against liability for OSPs who act as merely passive conduits for infringing information and without

²⁸⁰⁷ Sega Enterprises Ltd. v. Sabella, 1997 Copyr. Law. Dec. ¶ 27,648 (N.D. Cal. Dec. 18, 1996).

²⁸⁰⁸ Playboy Enterprises, Inc. v. Hardenburgh, Inc., 982 F. Supp. 503 (N.D. Ohio 1997).

knowledge of the infringement. These safe harbors may provide a defense against liability in certain instances to claims of contributory liability.

3. Vicarious Liability

A party may be vicariously liable for the infringing acts of another if it (1) has the right and ability to control the infringer's acts and (2) receives a direct financial benefit from the infringement.²⁸⁰⁹ Unlike contributory infringement, knowledge is not an element of vicarious liability.²⁸¹⁰

(a) The Netcom Case and its Progeny

In the Netcom case, the court refused to impose liability on Netcom under a theory of vicarious liability. The court found that there was a genuine issue of material fact as to whether Netcom had the right and ability to control the activities of its subscribers, in view of the fact that Netcom's expert testified that with an easy software modification Netcom could identify postings containing particular words or from particular individuals, and Netcom had acted to suspend subscribers' accounts on over one thousand occasions.²⁸¹¹

However, the court held that the second prong of the test was not satisfied, because there was no evidence that Netcom received a direct financial benefit from the infringing postings, or that such postings enhanced the value of Netcom's services to subscribers or attracted new subscribers.²⁸¹²

In refusing to impose vicarious liability because it found Netcom received no direct financial benefit from the infringing postings, the court in Netcom relied on the district court's decision in Fonovisa, Inc. v. Cherry Auction, Inc.,²⁸¹³ which found no direct financial benefit despite an argument that lessees at a swap meet included many vendors selling counterfeit goods and that clientele sought "bargain basement prices."²⁸¹⁴ It should be noted that the Ninth Circuit subsequently reversed Fonovisa, and appears to have adopted a less demanding standard for financial benefit for purposes of vicarious liability, which may undermine the strength of the

²⁸⁰⁹ E.g., Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 306 (2d Cir. 1963).

²⁸¹⁰ Religious Technology Center v. Netcom On-Line Communication Servs., 907 F. Supp. 1361, 1375 (N.D. Cal. 1995); R. Nimmer, *Information Law* ¶ 4.11, at 4-40 (2001).

²⁸¹¹ Religious Technology Center v. Netcom On-Line Communication Servs., 907 F. Supp. 1361, 1376 (N.D. Cal. 1995).

²⁸¹² Id. at 1377. The plaintiffs argued that the financial benefit prong was satisfied based on "Netcom's advertisements that, compared to competitors like CompuServe and America Online, Netcom provides easy, regulation-free Internet access. Plaintiffs assert that Netcom's policy attracts copyright infringers to its system, resulting in a direct financial benefit. The court is not convinced that such an argument, if true, would constitute a direct financial benefit to Netcom from *Erlich's* infringing activities." Id. (emphasis in original).

²⁸¹³ 847 F. Supp. 1492 (E.D. Cal. 1994).

²⁸¹⁴ Id. at 1496.

Netcom decision as precedent on this point. The Ninth Circuit held that adequate financial benefit was alleged by virtue of the fact that the operator of the swap meet received financial benefits through admission fees, parking fees, and sales at concession stands.²⁸¹⁵ A copyright holder seeking to hold an OSP or BBS operator vicariously liable might argue under Fonovisa that the subscription fees paid by the infringers should be sufficient financial benefit, just as were the admission fees, parking fees, and concession stand sales in Fonovisa. In addition, as discussed above, in the Napster case, the Ninth Circuit ruled that Napster had received a financial benefit because the presence of infringing material on the Napster system acted as a draw for users.

The Ninth Circuit's holdings in both Fonovisa and Napster suggest a standard that does not require direct financial benefit from the infringing activity itself, but rather that the infringing activity contributes to an overall commercial design and benefit for the operator.²⁸¹⁶

In one decision handed down after both the Netcom and Fonovisa decisions, Marobie-FL, Inc. v. National Association of Fire Equipment Distributors,²⁸¹⁷ the court, citing the Netcom case, refused to hold vicariously liable an OSP supplying Internet service to a website that contained infringing material because the infringements that occurred through the website did not directly financially benefit the OSP. The website owner paid the OSP a flat quarterly subscription fee that did not change based upon how many people visited the website or what was accessed on such site.²⁸¹⁸

(b) The Napster Cases

(For a discussion of vicarious liability in the Napster cases, see Section III.C.2.(c)(1) above.)

(c) Ellison v. Robertson

(For a discussion of vicarious liability in the case of Ellison v. Robertson, see Section III.C.6(b)(1)(i) below.)

(d) Perfect 10 v. Cybernet Ventures

The facts of the case of Perfect 10, Inc. v. Cybernet Ventures, Inc.²⁸¹⁹ are set forth in Section III.C.2(f) above. In that case, the court found, on a motion for a preliminary injunction, that the plaintiff had established a strong likelihood of success on its claim of vicarious liability. The court ruled that the defendant Cybernet had a direct financial interest in the infringing activities of its member sites because Cybernet benefited from such sites to the extent they

²⁸¹⁵ Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996).

²⁸¹⁶ R. Nimmer, Information Law ¶ 4.13[2], at 4-49 (2001).

²⁸¹⁷ 45 U.S.P.Q.2d 1236 (N.D. Ill. 1997).

²⁸¹⁸ Id. at 1245.

²⁸¹⁹ 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

acted as a draw for new subscribers to Cybernet's service. The court further noted that the relationship between Cybernet and its member sites was so close that it appeared to Cybernet's subscribers as if the Cybernet service constituted a single brand. In addition, subscribers paid all the money for their subscription fees directly to Cybernet, which then apportioned it to the member sites as commissions.²⁸²⁰

With respect to the control prong, the court found that Cybernet had the ability to control its member sites. Cybernet had a monitoring program in place under which its member sites received detailed instructions regarding issues of layout, appearance and content. Cybernet monitored images on the sites to make sure that celebrity images did not over-saturate the content found within the sites making up Cybernet's service. Cybernet also forbade its members sites to display certain types of images. Accordingly, the court concluded that Cybernet had sufficient control over the infringing activity to be vicariously liable.²⁸²¹

(e) The Aimster/Madster Lawsuits

The facts of the case of Aimster/Madster lawsuits are set forth in Section III.C.2(c)(3) above. In that case, the district court found, on a motion for a preliminary injunction, that the plaintiffs had established a reasonable likelihood of success on their claim of vicarious liability. The court ruled that Aimster had the right and ability to supervise its users merely because it retained the right under its Terms of Service to terminate service to individual users who were repeat violators of copyright law – as required by the DMCA safe harbors, thereby raising the Catch 22 discussed in Section III.C.2(c)(1).10 above in connection with the Napster case, which Catch 22 led the courts in the Hendrickson v. eBay, CoStar, and Perfect 10 v. Cybernet Ventures cases to reject this interpretation (see Sections III.C.6(b)(1)(iii).b, c & d below). In addition, Aimster controlled access of its users by requiring them to log on after paying their monthly fee to join Club Aimster. The court rejected the argument that the encryption on the Aimster system effectively prevented Aimster from controlling the activity of its users, ruling that Aimster need not, as a matter of law, have the physical Internet address of its users in order to be deemed to have sufficient right and ability to control them.²⁸²² "The fact that users must log in to the system in order to use it demonstrates that Defendants know full well who their users are."²⁸²³

The district court also concluded that the defendants had a direct financial interest in the infringing activities of Aimster users, because each Club Aimster user was required to pay \$4.95 per month to use the service, and there was evidence that every Aimster was now required to pay the fee. In addition, citing Napster II, the court ruled that the financial benefit element was

²⁸²⁰ Id. at 1171-72.

²⁸²¹ Id. at 1173.

²⁸²² In re Aimster Copyright Litigation, 252 F. Supp. 2d 634, 654-55 (N.D. Ill. 2002).

²⁸²³ Id. at 655.

satisfied because the existence of infringing activities acted as a draw for potential customers to the system.²⁸²⁴

On appeal, the Seventh Circuit stated that it was “less confident” than the district judge was that the plaintiffs were likely to prevail on the vicarious infringement theory.²⁸²⁵ Judge Posner noted that vicarious liability could conceivably have been applied in the Sony case given that the Court treated vicarious and contributory infringement interchangeably, and Sony could have made a design change in its product that would have controlled its users’ ability to fast forward through commercials, which Judge Posner found to be the creation of infringing derivative works.²⁸²⁶ However, he concluded that the court need not reach the issue because Aimster’s “ostrich-like refusal” to eliminate the encryption feature in its system and “discover the extent to which its system was being used to infringe copyright” made it a contributory infringer, and that was a sufficient basis to affirm the grant of the preliminary injunction without reaching the vicarious liability issue.²⁸²⁷

(f) The StreamCast/Kazaa/Grokster Lawsuits

The facts of the case of StreamCast/Kazaa/Grokster lawsuits are set forth in Section III.C.2(c)(4) above. In that case, the court granted summary judgment to the defendants StreamCast and Grokster on the plaintiff’s claim for vicarious liability. With respect to the financial benefit prong, the court ruled that both defendants derived a financial benefit from the infringing conduct of the users of their software, since the ability to trade copyrighted songs and other copyrighted works acted as a “draw” for many users of the software. The defendants also derived substantial revenue from advertising displayed through the software.²⁸²⁸

With respect to the control prong, the court distinguished the Napster system, in which centralized search indices and mandatory registration system gave Napster both knowledge of what was being exchanged and the ability to police those exchanges. By contrast, the court found no evidence before it that the defendants had the ability to supervise and control the infringing conduct, all of which occurred after the product had passed to end-users.²⁸²⁹

The plaintiffs argued that the defendants’ software could have been altered to prevent users from sharing copyrighted files and the court should require such alterations, as the Ninth Circuit required Napster to do. The plaintiffs noted that the defendants’ software already included optional screens for pornographic/obscene file names and that it could just as easily screen out copyrighted song titles. The plaintiffs also argued that an effective “meta data”

²⁸²⁴ Id.

²⁸²⁵ In re Aimster Copyright Litigation, 334 F.3d 643, 654 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004).

²⁸²⁶ Id. at 647, 654.

²⁸²⁷ Id. at 654-55.

²⁸²⁸ Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029, 1043-44 (C.D. Cal. 2003).

²⁸²⁹ Id. at 1044-45.

screen could be implemented, as well as emerging “digital fingerprinting” technology.²⁸³⁰ In a significant holding, the court rejected these arguments, stating that “whether these safeguards are practicable is immaterial to this analysis, as the obligation to ‘police’ arises only where a defendant has the ‘right and ability’ to supervise the infringing conduct.”²⁸³¹ Unlike Napster, whose client software was an essential component of the integrated Napster system, the defendants provided software that communicated across networks entirely outside defendants’ control.²⁸³² “The doctrine of vicarious infringement does not contemplate liability based upon the fact that a product could be made such that it is less susceptible to unlawful use, where no control over the user of the product exists.”²⁸³³ Accordingly, the court granted the defendants summary judgment on the issue of vicarious liability.

On appeal, the Ninth Circuit affirmed.²⁸³⁴ The Ninth Circuit began by observing that it had held in the first appeal of the Napster case that the Sony doctrine has no application to vicarious infringement because vicarious liability was not before the Supreme Court in that case. Noting further that the issue of direct financial benefit, via advertising revenue, was undisputed, the court turned its analysis to the prong of right and ability to supervise the infringers.²⁸³⁵

Noting that the Napster case had found especially important the fact that Napster had an express policy reserving the right to block infringers’ access to its system, the court contrasted the instant case in which there was no evidence in the record to establish that either of the defendants had the ability to block access to individual users. Although Grokster nominally reserved the right to terminate access, StreamCast did not maintain a licensing agreement with persons who downloaded Morpheus. Given the lack of a registration and log-in process, however, even Grokster had no ability to actually terminate access to filesharing functions, absent a mandatory software upgrade to all users that the particular user refused, or IP address-blocking attempts (which would not be effective against most users who were utilizing dynamic IP addresses). The court also noted that none of the communication between the defendants and users provided a point of access for filtering or searching for infringing files, since infringing material and index information did not pass through the defendants’ computers.²⁸³⁶

In the case of StreamCast, shutting down its XML file altogether would not prevent anyone from using the Gnutella network. In the case of Grokster, its licensing agreement with Kazaa/Sharman did not give it the ability to mandate that root nodes be shut down. In any event, the court noted that any alleged ability to shut down operations altogether would be more akin to the ability to close down an entire swap meet than the ability to exclude individual

²⁸³⁰ Id. at 1045.

²⁸³¹ Id. (emphasis in original).

²⁸³² Id.

²⁸³³ Id. at 1045-46.

²⁸³⁴ Metro-Goldwyn-Mayer v. Grokster, 380 F.3d 1154 (9th 2004).

²⁸³⁵ Id. at 1164.

²⁸³⁶ Id. at 1165.

participants or to police aisles. The Ninth Circuit noted that the district court had correctly characterized the copyright owners' evidence of the right and ability to supervise as little more than a contention that the software itself could be altered to prevent users from sharing copyrighted files.²⁸³⁷

In arguing that this ability constitutes evidence of the right and ability to supervise, the Copyright Owners confuse the right and ability to supervise with the strong duty imposed on entities that have already been determined to be liable for vicarious copyright infringement; such entities have an obligation to exercise their policing powers to the fullest extent, which in Napster's case included implementation of new filtering mechanisms. ... But the potential duty a district court may place on a vicariously liable defendant is not the same as the "ability" contemplated by the "right and ability to supervise" test. ... We agree with the district court that possibilities for upgrading software located on another person's computer are irrelevant to determining whether vicarious liability exists.²⁸³⁸

Accordingly, the court affirmed summary judgment for the defendants on the vicarious liability claim.²⁸³⁹

(g) Perfect 10 v. Visa International

In Perfect 10, Inc. v. Visa International Service Ass'n,²⁸⁴⁰ Perfect 10, owner of the copyrights in pornographic materials, sought to hold various credit card and banking institutions liable for contributory and vicarious infringement for providing financial services to various web sites that Perfect 10 alleged contained infringing copies of its copyrighted materials. The district court granted the defendants' motion to dismiss.

Perfect 10 argued that the defendants had the right and ability to control the infringing activities because (i) provision of financial services was essential to the survival of the allegedly infringing web sites, and the defendants could therefore dictate content by threatening to revoke their services if the web sites did not comply with their standards, and (ii) the defendants had in place internal regulations governing the provision of service to high-risk merchants, including adult entertainment web sites. The district court rejected both arguments. As to the first, the court noted that the record established the allegedly infringing web sites would be able to continue their alleged infringing conduct regardless of whether the defendants blacklisted

²⁸³⁷ Id. at 1165-66.

²⁸³⁸ Id. at 1166. The plaintiffs also argued that Grokster and StreamCast should not be able to escape vicarious liability by turning a "blind eye" to the detectable infringement of their users. The Ninth Circuit rejected this argument, stating that there is no separate "blind eye" theory or element of vicarious liability that exists independently of the traditional elements of liability. Id.

²⁸³⁹ Id. at 1167. On appeal, the Supreme Court did not reach the issue of vicarious liability in view of its resolution of the case under the doctrine of inducement.

²⁸⁴⁰ 71 U.S.P.Q.2d 1914 (N.D. Cal. 2004), aff'd, 494 F.3d 788 (9th Cir. 2007), cert. denied, 553 U.S. 1079 (2008).

them. As to the second, even if the defendants had internal regulations requiring monitoring of web sites, the web sites were not bound by such regulations and the defendants had no contractual right to dictate the web sites' content or to take action against them in the event of infringing activity. And unlike the Fonovisa swap meet case, the defendants could not "eject" the web sites from the Internet. Accordingly, the district court ruled that the defendants had no way to control the infringing conduct of the web sites.²⁸⁴¹

The court noted that the complaint included facts that might indicate a financial benefit to the defendants as a result of the draw from the alleged infringing images, but because of the absence of a right or ability to exercise control over the alleged infringing activity, the existence of a financial benefit would not be sufficient to establish vicarious liability. Accordingly, the district court granted the defendants' motion to dismiss the claim with leave to Perfect 10 to amend.²⁸⁴²

On appeal, the Ninth Circuit affirmed.²⁸⁴³ The Ninth Circuit agreed with the district court that the rules and regulations of the defendants prohibiting member banks from providing services to merchants engaging in certain illegal activities and requiring member banks to investigate merchants suspected of engaging in such illegal activities were insufficient to establish the right and ability to control infringing activity for purposes of vicarious liability. The court noted that the defendants did not have any ability to directly control the infringing activity occurring on the web sites at issue, and the court held that the mere ability to withdraw a financial carrot did not constitute the right and ability to control infringing activity that vicarious infringement requires.²⁸⁴⁴

The court rejected Perfect 10's analogy to the Napster case on the ground that the defendants, like Napster, had the ability to policy their systems and failed to exercise that right to prevent the exchange of copyrighted material. The court noted that Napster's policing power was much more intimate and directly intertwined with the infringing activity than the defendants' payment systems. Napster could block users' access to its system and thereby deprive particular users of use of its location and distribution tools. By contrast, although the defendants could block access to their payment system, they could not themselves block access to the Internet, to any particular web sites, or to search engines enabling the location of such web sites. Nor could the defendants take away the tools the offending web sites used to reproduce, alter, and distribute the infringing images over the Internet.²⁸⁴⁵

Finally, the court rejected Perfect 10's argument that the defendants' rules and regulations imposed on merchant banks gave them contractual control over the content of their

²⁸⁴¹ Id. at 1918.

²⁸⁴² Id.

²⁸⁴³ Perfect 10, Inc. v. Visa International, 494 F.3d 788 (9th Cir. 2007), cert. denied, 553 U.S. 1079 (2008).

²⁸⁴⁴ Id. at 802-03.

²⁸⁴⁵ Id. at 803-04.

merchants' web sites sufficient for vicarious liability. The court held that the ability to exert financial pressure did not give the defendants the right or ability to control the actual infringing activity taking place on the web sites. The court found the defendants analogous to Google, which was held not liable in the Perfect 10 v. Amazon case for vicarious infringement even though search engines could effectively cause a web site to disappear by removing it from their search results, and reserved the right to do so.²⁸⁴⁶ In sum, although the infringing activities at issue might not be profitable without access to the defendants' credit card payment systems, the court held that the "alleged infringement does not turn on the payment; it turns on the reproduction, alteration and distribution of the images, which Defendants do not do, and which occurs over networks Defendants do not control."²⁸⁴⁷ Accordingly, because Perfect 10 had failed to establish the control prong, it had not pled a viable claim of vicarious liability, and the court ruled that it need not reach the issue of direct financial interest.²⁸⁴⁸

The Ninth Circuit's rulings were clearly heavily influenced by policy considerations and a belief that to hold tertiary financial service providers secondarily liable for infringing activities on web sites for which they processed payments would simply go too far. Indeed, the court began its analysis of the secondary liability issues with the following:

We evaluate Perfect 10's claims with an awareness that credit cards serve as the primary engine of electronic commerce and that Congress has determined it to be the "policy of the United States – (1) to promote the continued development of the Internet and other interactive computer services and other interactive media [and] (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation."²⁸⁴⁹

(h) Parker v. Google

In Parker v. Google,²⁸⁵⁰ pro se plaintiff Gordon Parker was the owner of copyright in an e-book titled "29 Reasons Not To Be A Nice Guy." He posted Reason # 6 on USENET. Parker asserted that Google's automatic archiving of this USENET content made Google vicariously liable for copyright infringement because it facilitated users to make unauthorized distributions and copies of his copyrighted material through Google's web site, and Google had the right and ability to supervise or control such user activity and received a substantial financial benefit from it in the form of advertising revenue and goodwill. The district court rejected this argument for two reasons. First, Parker had failed to allege infringement of any specific registered works that were infringed, nor had he alleged specific conduct by a third party that Google may have had the right and ability to supervise. Second, his broad allegations that Google's advertising

²⁸⁴⁶ Id. at 804-05.

²⁸⁴⁷ Id. at 806.

²⁸⁴⁸ Id. at 806.

²⁸⁴⁹ Id. at 794 (quoting 47 U.S.C §§ 230(b)(1), (2)).

²⁸⁵⁰ 422 F. Supp. 2d 492 (E.D. Pa. 2006), aff'd, 2007 U.S. App. LEXIS 16370 (3d Cir. July 10, 2007).

revenue was directly related to the number of Google users was insufficient to maintain a claim of vicarious liability, as it did not allege any actual relationship between infringing activity and the number of users that would demonstrate an obvious and direct financial interest in infringing activity.²⁸⁵¹ On appeal, the Third Circuit affirmed in an unpublished decision for the reasons articulated by the district court.²⁸⁵²

(i) **Louis Vuitton v. Akanoc Solutions**

In Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.,²⁸⁵³ the defendants provided OSP services that hosted websites through which the plaintiff alleged goods were being sold that infringed its trademarks and copyrights. The plaintiff sought to hold the defendants contributorily and vicariously liable for hosting such websites and the defendants moved for summary judgment. The court denied the motion as to contributory infringement, but granted it as to vicarious infringement.²⁸⁵⁴ With respect to vicarious liability, the plaintiff argued that the ability to infringe without strict policing by the defendants acted as a draw to the site, in conjunction with the defendants' Chinese language skills and competitive technology. The court rejected this argument, noting that the plaintiff had provided no evidence that any of the defendants' customers used their services because of the ability to infringe.²⁸⁵⁵ The court also found that the plaintiff had not established a showing of direct financial benefit from infringing activity. "Plaintiff does not offer any evidence showing that Defendants made more money when they allowed infringement to continue or less money when they did not. Nor does Plaintiff offer any evidence showing that customers sought or abandoned Defendants' services based on their ability to infringe. Furthermore, Plaintiff concedes that Defendants have 'unplugged' infringers in the past. By doing so, Plaintiff undermines its own contention that Defendants turn a blind eye to the infringing activity occurring on their servers."²⁸⁵⁶

(j) **Live Face on Web v. Howard Stern Productions**

In Live Face on Web, LLC v. Howard Stern Productions, Inc.,²⁸⁵⁷ the plaintiff alleged that the defendant had infringed its copyright in proprietary software that allowed a company to display a "live" salesperson or spokesperson superimposed on the company's web site. The plaintiff's allegations that the unauthorized presentations on the defendant's web site were designed to and did draw and prolong visitors' attention to the web site and to other Howard Stern media promoted on the web site, that the presentations increased the amount of time

²⁸⁵¹ Id. at 499-500.

²⁸⁵² Parker v. Google, 2007 U.S. App. LEXIS 16370 (3d Cir. July 10, 2007).

²⁸⁵³ 591 F. Supp. 2d 1098 (N.D. Cal. 2008), aff'd in part & rev'd in part, 658 F.3d 936 (9th Cir. 2011).

²⁸⁵⁴ Id. at 1113. The court's rulings with respect to contributory infringement are set forth in Section III.C.2(j) above.

²⁸⁵⁵ Id. at 1109-10.

²⁸⁵⁶ Id. at 1110-11 (citations omitted). For subsequent proceedings in this case, including the Ninth Circuit's rulings on appeal, see Sections III.C.1(a) and III.C.2(j) above.

²⁸⁵⁷ 2009 U.S. Dist. LEXIS 21373 (E.D. Pa. 2009).

users would spend on the web site, and that the presentations enhanced visitors' online experience, thus reinforcing and advancing the brand and image of the Howard Stern Show and the defendant's products and services, were sufficient allegations of direct financial interest to avoid a motion to dismiss the plaintiff's claim for vicarious liability.²⁸⁵⁸

(k) Arista Records v. Usenet.com

In Arista Records LLC v. Usenet.com, Inc.,²⁸⁵⁹ the court applied both prongs of the vicarious liability doctrine in a rather broad fashion, in a factual context that was admittedly ripe for imposing liability. In that case, the defendants operated a Napster-like Usenet service that advertised to and targeted users who wanted to download music files. Unlike peer-to-peer filing sharing networks, the files were stored on "spool" news servers operated by the defendants. The defendants created designated servers for newsgroups containing music binary files to increase their retention time over other types of Usenet files.²⁸⁶⁰ The court granted the plaintiffs' motion for summary judgment on their claim for vicarious liability. Citing the Supreme Court's Grokster decision, the court noted that one may be vicariously liable if he has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities. The court found that the defendants earned a direct financial benefit from the infringement because their revenues increased depending on their users' volume of downloads, the majority of which had been shown to be infringing. The court noted also that the infringing content on the service acted as a draw for users to subscribe to the service. The court rejected the defendants' argument that they lacked direct financial benefit from infringement because they were paid on a per-volume, not per-download, basis and because infringing music accounted for less than 1% of the newsgroups available on their service. The court noted that under the law, the draw of infringement need not be the primary, or even a significant, draw – rather it need only be "a" draw.²⁸⁶¹

The court ruled that the defendants had also failed to exercise their right and ability to stop or limit infringement on their service. The defendants had in the past exercised their right and ability to control their subscribers' actions by terminating or limiting access of subscribers who posted spam, restricted download speeds for subscribers who downloaded a disproportionate volume of content, and taken measures to restrict users from posting or downloading files containing pornography.²⁸⁶² "Defendants likewise have the right and ability to block access to articles stored on their own servers that contain infringing content, but the record does not show any instance of Defendants exercising that right and ability to limit infringement by its users. More generally, Defendants have the right and ability to control which newsgroups to accept and maintain on their servers and which to reject, an ability they chose to

²⁸⁵⁸ Id. at *11-12.

²⁸⁵⁹ 633 F. Supp. 2d 124 (S.D.N.Y. 2009).

²⁸⁶⁰ Id. at 130-31.

²⁸⁶¹ Id. at 156-57.

²⁸⁶² Id. at 157.

exercise when they disabled access to approximately 900 music-related newsgroups in 2008.”²⁸⁶³ Accordingly, the court found the defendants vicariously liable.²⁸⁶⁴

(l) Corbis v. Starr

In Corbis Corp. v. Starr,²⁸⁶⁵ the defendant Master, a janitorial maintenance company, hired defendant West Central, an Internet services company, to redesign and host its web site. The redesigned site contained four unauthorized images owned by the plaintiff Corbis. Corbis sent a letter to Master notifying it of the infringing images, and Master responded by directing West Central to remove the images, which West Central did. Corbis then filed suit against the defendants for copyright infringement and moved for summary judgment. The court found West Central directly liable as a matter of law for copying the images onto Master’s web site. It also found Master vicariously liable as a matter of law. The control prong of vicarious liability was satisfied because Master had the power to approve changes that West Central made to its corporate web site, including whether photos were used, and also had the ability to stop or limit infringing uses. West Central received a financial benefit from the infringement because the use of the copyrighted images (three of which depicted janitorial and cleaning services) helped draw customers.²⁸⁶⁶

(m) Arista Records v. Lime Group

(For a discussion of vicarious liability in this case, see Section III.C.4(d) below.)

(n) Hermeris v. Brandenburg

(For a discussion of vicarious liability in this case, see Section III.C.2(l) above.)

(o) Luvdarts v. AT&T Mobility

In Luvdarts LLC v. AT&T Mobility, LLC,²⁸⁶⁷ the court ruled on a motion to dismiss that the defendant wireless carriers had no vicarious liability for operation of a system that enabled sharing of mobile multimedia messaging (MMS) content between devices, including the plaintiffs’ copyrighted electronic greeting messages, because the plaintiffs had not plausibly alleged that the defendants had the right or ability to filter the content transmitted on their wireless networks. In addition, the court noted that the plaintiffs had designed their “Luvdarts” mobile multimedia messaging content several years after the defendants designed their mobile multimedia messaging system.²⁸⁶⁸ “The court is not aware of any authority that would require

²⁸⁶³ Id.

²⁸⁶⁴ Id.

²⁸⁶⁵ 2009 U.S. Dist. LEXIS 79626 (N.D. Ohio Sept. 2, 2009).

²⁸⁶⁶ Id. at *2 & *7-9.

²⁸⁶⁷ 2011 U.S. Dist. LEXIS 28369 (C.D. Cal. Mar. 17, 2011), aff’d, 710 F.3d 1068 (9th Cir. 2013).

²⁸⁶⁸ Id. at *9, 11.

Defendants to retrofit their general purpose network to accommodate technology later developed by a third-party for the purpose of being transmitted with that very technology.”²⁸⁶⁹ The court also dismissed the plaintiffs’ claims for inducement and contributory infringement because the plaintiffs had not alleged that the defendants’ networks were designed with the object of promoting infringement or that the defendants had taken affirmative steps to actively encourage or induce infringement, and the defendants’ wireless networks were capable of noninfringing uses.²⁸⁷⁰

On appeal, the Ninth Circuit affirmed.²⁸⁷¹ With respect to vicarious liability, the court noted that Luvdarts conceded that the defendant carriers had no way of supervising the use of their networks for copyright infringement. Instead, Luvdarts’ complaint alleged only that the carriers could establish a system that would give them the right and ability to supervise the infringing activity. Luvdarts argued that this allegation was sufficient to survive a motion to dismiss.²⁸⁷² The court rejected this argument, noting that “under contributory liability the Carriers’ failure to implement a digital rights management system may be used as circumstantial evidence of ‘the object of promoting’ infringement. See *Grokster*, 545 U.S. at 936-37. But under vicarious liability, it cannot substitute for an allegation of a capacity to supervise. Luvdarts’s failure to allege that the Carriers have at least something like a capacity to supervise is fatal to a claim of vicarious liability. Even if the doctrine of vicarious liability imposed some affirmative duty to acquire supervisory capacity, Luvdarts has failed to allege facts that plausibly show that the Carriers could implement an effective system.”²⁸⁷³

With respect to contributory liability, the court noted that Luvdarts had failed to allege that the carriers had the requisite specific knowledge of infringement. The notices of infringement that Luvdarts had sent to the defendants were insufficient to establish specific knowledge because they were merely 150-page-long lists of titles, apparently just a transcription of every title copyrighted by Luvdarts, stating that Luvdarts wanted “accountability” for the unauthorized distribution of those titles. The notices did not identify which of the titles were infringed, who infringed them, or when the infringement occurred and therefore did not satisfy Section 512 of the DMCA, by which the notices purported to be governed.²⁸⁷⁴

The court also rejected Luvdarts’ argument that the carriers were willfully blind to the infringement that was occurring, because Luvdarts had not alleged that the carriers took active steps to avoid acquiring infringing knowledge. The most it had alleged was that the carriers proceeded with the development and operation of the MMS networks indifferent to the risk of copyright infringement, which was insufficient to meet the standard of willful blindness.

²⁸⁶⁹ *Id.* at *10-11.

²⁸⁷⁰ *Id.* at *7.

²⁸⁷¹ *Luvdarts LLC v. AT&T Mobility, LLC*, 710 F.3d 1068 (9th Cir. 2013).

²⁸⁷² *Id.* at 1071.

²⁸⁷³ *Id.* at 1071-72.

²⁸⁷⁴ *Id.* at 1072-73.

Accordingly, the court ruled that the district court had properly dismissed Luvdarts' complaint with prejudice.²⁸⁷⁵

(p) Flava Works v. Gunter

The facts of this case are set forth in Section III.C.1(b) above. The court granted the defendants' motion to dismiss the plaintiff's claim for vicarious liability. With respect to the control requirement, the court noted that all the plaintiff had alleged as the basis that the defendants had the right and ability to control the infringing activity was that it had ownership of and operated the myVidster site. Mere ownership and control of the site was insufficient to establish the right and ability to control infringing activity on the site. With respect to the financial benefit requirement, the court noted that all the plaintiff needed to allege was that the availability of infringing material on myVidster was a draw for customers. However, the plaintiff had failed to do so. Although the complaint alleged that inexpensive storage space and the ability to share videos attracted customers to myVidster, it did not allege that the presence of the infringing material on the site enhanced the site's attractiveness or drew customers. Accordingly, the court dismissed the claim for vicarious infringement.²⁸⁷⁶

(q) Perfect 10 v. Giganews

(For a discussion of vicarious liability issues in this case, see Section III.C.2(n) above.)

(r) Masck v. Sports Illustrated

(For a discussion of vicarious liability issues in this case, see Section III.C.2(o) above.)

(s) Disney Enterprises v. Hotfile

The facts of this case are set forth in Section III.C.6(b)(1)(iii).y below. With respect to the plaintiffs' claim of vicarious liability and the requirement of financial benefit, Hotfile acknowledged that infringing files drove some amount of revenues to Hotfile. The connection between infringement and sales was further evidenced by a dramatic drop in Hotfile's income after the complaint was filed and Hotfile implemented a three-strikes policy and technologies to ferret out infringers. Even if infringement was not central to its success, the court found it undeniable that Hotfile financially benefitted from infringement by attracting some users, which was sufficient to satisfy the financial benefit prong.²⁸⁷⁷

With respect to the control prong, the court rejected Hotfile's argument that it could not determine which files on its system were infringing. The court cited authority that courts have viewed the control prong expansively under common law, finding that service providers have the

²⁸⁷⁵ Id. at 1073.

²⁸⁷⁶ Flava Works, Inc. v. Gunter, 2011 U.S. Dist. LEXIS 50067 at *13-16 (N.D. Ill. May 10, 2011), rev'd on other grounds, 689 F.3d 754 (7th Cir. 2012).

²⁸⁷⁷ Disney Enterprises, Inc. v. Hotfile Corp., 2013 U.S. Dist. LEXIS 172339 at *128-29 (S.D. Fla. Sept. 20, 2013).

capacity to control the activities of their users simply by virtue of providing the means to commit direct infringement. In any event, in this case, Hotfile controlled the means of infringement by, among other things, mandating user registration and hosting the infringing materials on its own servers. In addition, Hotfile had a stated policy that permitted it to control user activity and to exclude users, and maintained that it had exercised that control in policing content. Hotfile had also adopted technology that it claimed was effective in filtering and targeting infringing works. The court found that these actions therefore belied Hotfile's argument that it lacked control because it had no search function and no way to identify or remove infringing files. Hotfile had failed to properly exercise its control in view of the number of users who were blatantly infringing. Accordingly, the court granted summary judgment to the plaintiffs on their claim of vicarious liability.²⁸⁷⁸

In Dec. 2013, the MPAA announced a settlement under which the district court had awarded damages of \$80 million to the plaintiffs and ordered Hotfile to either shut down its operations or use digital fingerprinting technology to prevent copyright infringement by its users.²⁸⁷⁹

(t) Capitol Records v. Escape Media

(For a discussion of vicarious liability issues in this case, see Section III.C.1(c) above.)

(u) UMG Recording v. Escape Media

(For a discussion of vicarious liability issues in this case, see Section III.C.1(d) above.)

(v) Gardner v. CafePress

(For a discussion of vicarious liability issues in this case, see Section II.A.4(bb) above.)

(w) BMG v. Cox Communications

(For a discussion of vicarious liability issues in this case, see Section III.C.2(w) above.)

(x) GC2 v. Int'l Game Tech.

In GC2 Inc. v. Int'l Game Tech. PLC,²⁸⁸⁰ the court issued an interesting ruling with respect to claims for vicarious copyright infringement brought by the plaintiff against the defendants for their unauthorized use of the plaintiff's copyrighted artwork in online games distributed by the

²⁸⁷⁸ Id. at *129-134. The court also found one of Hotfile's founders, who was deeply involved in all aspects of the business, personally liable for Hotfile's vicarious liability. Id. at *134-147.

²⁸⁷⁹ "Hotfile To Pay \$80M to MPAA, Studios In Copyright Suit," *Law360* (Dec. 3, 2013), available as of Dec. 7, 2013 at http://www.law360.com/ip/articles/493076?nl_pk=be5fde4e-8dc1-4d81-b621-f0352bcdff74&utm_source=newsletter&utm_medium=email&utm_campaign=ip.

²⁸⁸⁰ 255 F. Supp. 3d 812 (N.D. Ill. 2017).

defendants. Specifically, the court ruled that the software license agreements some of the defendants had with their end users governing the online games were sufficient to support allegations that the defendants' had the ability to control their end users. Under the license agreements, the defendants had the authority to terminate the license or to bring a lawsuit where the end user violated the terms of the agreement. The court read these provisions as sufficient, for purposes of denying a motion to dismiss, to support the plaintiff's allegation that the defendants had the authority to put a stop to the infringing conduct even after a consumer's one-time purchase of the game.²⁸⁸¹ For a deeper discussion of this case, see Section II.G.1(b)(2)(ii).f above.

(y) VHT v. Zillow Group

(For a discussion of vicarious liability issues in this case, see Section III.C.1(i) above.)

(z) UMG Recordings v. Grande Communications Networks

(For a discussion of vicarious liability issues in this case, see Section III.C.2(aa) above.)

(aa) Erickson Prods v. Kast

(For a discussion of vicarious liability issues in this case, see Section III.C.2(cc) above.)

(bb) UMG Recordings v. Bright House Networks

A group of plaintiff record companies sought to hold Internet service provider Bright House Networks (BHN) liable for refusing to take steps to stop its subscribers from illegally downloading and distributing the plaintiffs' music through BitTorrent and other file-sharing software. The plaintiffs alleged that BHN's consumer marketing material touted how its service enabled subscribers to download and upload large amounts of content, including music, in seconds, and that BHN refused to terminate or otherwise take action against subscribers who allegedly infringed the plaintiff's works.²⁸⁸²

The court granted BHN summary judgment on the plaintiffs' vicarious liability claim on the ground that they had failed to adequately allege that BHN received a direct financial benefit from its users' infringing activity. The plaintiffs argued that BHN received such direct financial benefit because at least some percentage of BHN's customers were drawn to its service, at least in part, by the ability to infringe. The plaintiffs relied on a line of cases from other Circuits holding that, to constitute a direct financial benefit, the "draw" of infringement need not be the primary, or even a significant draw, but rather need only be a draw. The court declined to adopt that interpretation of direct financial benefit, finding that it effectively read the limiting term "direct" out of the test. Instead, the court concluded, citing among other cases the Supreme

²⁸⁸¹ Id. at 824-25.

²⁸⁸² UMG Recordings, Inc. v. Bright House Networks, LLC, 2020 U.S. Dist. LEXIS 122774 at *4-7 (M.D. Fla. July 8, 2020).

Court's Grokster case, that even if liability is to be established under a "draw" theory, liability must nonetheless be based upon a direct financial benefit to the alleged vicarious infringer. Thus, the plaintiff must be prepared to show, and must therefore allege, that the availability of infringing content provides the main customer draw to the service. Absent this limitation, the draw theory would provide essentially for the limitless expansion of vicarious liability into spheres far removed from the factual settings out of which vicarious liability originally arose. Moreover, requiring that the availability of infringing material be the primary customer draw to the service ensures that a defendant will be held liable only if it has an obvious and direct financial interest in the infringing conduct.²⁸⁸³

The court found that, at most, the plaintiff s alleged that access to infringing content generally available on the Internet is one of many reasons motivating some subscribers to enroll with any OSP. The plaintiffs did not allege that there was anything unique about the service SHN offered as a portal to the Internet or as a portal to the alleged illegal content. More generally, it was not readily apparent or plausibly alleged that an Internet thief would be drawn by the efficiency of Internet service any more than the average law-abiding purchaser of copyrighted content. The court noted that the plaintiffs had alternatively alleged that some subscribers were drawn in part to BHN by its failure to police infringing subscribers adequately, but stated that again that was not the test – the test is whether users are drawn to BHN by the availability of infringing content. Any proportionate value that might be ascribed by post hoc edict to the general enticement to purchase Internet services from BHN could not constitute a direct financial benefit to BHN owing principally to the draw to available infringing content. At best, any such benefit would be indirect and attenuated rather than obvious and direct. Lastly, the court observed that to accept the plaintiff's theory of vicarious liability would impose liability on every OSP, as the music at issue in the case was available on the Internet generally, as was the BitTorrent protocol, and was not something exclusively available through BHN's services.²⁸⁸⁴

(cc) Atari v. Redbubble

(For a discussion of this vicarious liability issues in this case, see Section III.C.1(j) above.)

4. Inducement Liability

(a) The Supreme Court's Grokster Decision

For a detailed discussion of the Supreme Court's Grokster decision, which formally introduced inducement liability into the copyright law for the first time, see Section III.C.2(c)(5) above.

²⁸⁸³ Id. at *14-17.

²⁸⁸⁴ Id. at *17-22.

(b) **Arista Records v. Usenet.com**

In Arista Records LLC. v. Usenet.com, Inc.,²⁸⁸⁵ the defendants operated a Napster-like Usenet service that advertised to and targeted users who wanted to download music files. Unlike peer-to-peer filing sharing networks, the files were stored on “spool” news servers operated by the defendants. The defendants created designated servers for newsgroups containing music binary files to increase their retention time over other types of Usenet files.²⁸⁸⁶ The court, although noting several courts that had expressed doubt as to whether inducement of infringement states a separate claim for relief, or whether it is a species of contributory infringement, granted the plaintiffs’ motion for summary judgment on their claim for inducement of infringement as a separate theory.²⁸⁸⁷

The court found the facts in the instant case very similar, and equally compelling, to those that led the Supreme Court to find inducement liability in Grokster. Specifically, a statistical survey based on random sampling concluded that over 94% of all content files offered in the defendants’ music-related binary newsgroups were infringing or highly likely to be infringing.²⁸⁸⁸ The defendants openly and affirmatively sought to attract former users of other notorious file-sharing services such as Napster and Kazaa, and boasted that as those file sharing services were scrutinized and shut down for copyright infringement, it would make the way for Usenet to “get back in the game.”²⁸⁸⁹ The defendants also used meta-tags such as “warez” and “Kazaa” in the source code of their website to ensure that a search on a search engine for illegal content would return their website as a result. The record was replete with evidence of the defendants’ own employees overtly acknowledging the infringing purpose for which their service was used and advertising such uses on their web site.²⁸⁹⁰ The defendants’ employees specifically provided technical assistance to users in obtaining copyrighted content and provided web site tutorials on how to download content, using infringing works as examples. Other evidence showed that, although the defendants had in place various tools and mechanisms that could be used to block access to infringing articles or newsgroups, they never used them to limit copyright infringement on their servers. Finally, the defendants’ graded subscription payment plan caused users to pay more the more they downloaded. Accordingly, the court concluded that the defendants’ intent to induce or foster infringement by its users on their services was unmistakable.²⁸⁹¹

²⁸⁸⁵ 633 F. Supp. 2d 124 (S.D.N.Y. 2009).

²⁸⁸⁶ Id. at 130-31.

²⁸⁸⁷ Id. at 150 n.17 & 154.

²⁸⁸⁸ Id. at 151-52.

²⁸⁸⁹ Id. at 152.

²⁸⁹⁰ Id. For example, an employee commented that the tag line for the service should be “piracy, porno and pictures – Usenet,” and another commented that “Usenet is full of Music and Movies so get your pirate on!” Id.

²⁸⁹¹ Id. at 153-54.

(c) Columbia Pictures v. Fung

The District Court Decision

In Columbia Pictures v. Fung,²⁸⁹² the defendants were operators of various sites that facilitated file sharing using the BitTorrent protocol. In a BitTorrent network, rather than downloading content files from an individual host, users of the network selected the content file they wished to download and then downloaded it in pieces through an automated process from a number of host computers (called a “swarm”) possessing the content (or portions of it) simultaneously. Servers called “trackers” managed the download process from the multiple hosts. The defendants’ sites (known as “torrent sites”) maintained indexes of files called “dot-torrent files” that contained information identifying the various hosts where pieces of the desired content were stored. Users could also upload dot-torrent files for use by others to locate desired content. The dot-torrent files did not contain the actual content users were searching for (such as a movie), but rather contained the data used by the BitTorrent client software on the user’s computer to retrieve the content through a simultaneous peer-to-peer transfer from the multiple hosts of the content.²⁸⁹³

The plaintiffs were the owners of copyrighted movies that could be searched for through the index of dot-torrent files on the defendants’ sites, then downloaded by users using the BitTorrent client software on their computers. They sought to hold the defendants secondarily liable for the downloading of infringing copies of their copyrighted content by users of the defendants’ sites. The court granted the plaintiffs summary judgment on the issue of liability based on a theory of inducement.²⁸⁹⁴

Because BitTorrent users could be scattered throughout the world, to establish liability for inducement, the plaintiffs needed to establish that instances of direct infringement by BitTorrent users had taken place in the United States. The court rejected the defendants’ argument the plaintiffs were required to provide evidence that both the transferor and the transferee of infringing content were located in the United States.²⁸⁹⁵ “[T]he acts of uploading and downloading are each independent grounds of copyright infringement liability. Uploading a copyrighted content file to other users (regardless of where those users are located) violates the copyright holder’s § 106(3) distribution right. Downloading a copyrighted content file from other users (regardless of where those users are located) violates the copyright holder’s § 106(1) reproduction right. Plaintiffs need only show that United States users either uploaded or

²⁸⁹² 2009 U.S. Dist. LEXIS 122661 (C.D. Cal. Dec. 21, 2009), aff’d, 710 F.3d 1020 (9th Cir. 2013).

²⁸⁹³ Id. at *8-11. “The dot-torrent file contains ‘hash’ values that are used to identify the various pieces of the content file and the location of those pieces in the network. The BitTorrent client application then simultaneously downloads the pieces of the content file from as many users as are available at the time of the request, and then reassembles the content file on the requesting computer when the download is complete.” Id. at *11-12.

²⁸⁹⁴ Id. at *3.

²⁸⁹⁵ Id. at *28-29.

downloaded copyrighted works; Plaintiffs need not show that a particular file was both uploaded and downloaded entirely within the United States.”²⁸⁹⁶ Plaintiffs had adequately provided sufficient evidence to establish acts of direct infringement in the United States through IP address data that located defendants’ users and showed that particular infringing downloads took place in the United States.²⁸⁹⁷

Turning to the facts of the case, the court granted the plaintiffs’ motion for summary judgment on the issue of inducement liability based on the following acts by the defendants:

– Defendants’ messages to users had stimulated others to commit infringement: The defendants web site had a “Box Office Movies” feature that periodically posted a list of the top 20 highest-grossing films then playing in the United States, which linked to detailed web pages concerning each film. Each of these pages contained “upload torrent” links allowing users to upload dot-torrent files for the films. The defendants’ web sites presented available torrent files, the vast majority of which pointed to infringing content, in browseable categories and provided further information about the content. The defendants also generated lists of the most popular files in categories like “Top 20 Movies.” The sites’ operator, Fung, made statements on the site encouraging or assisting infringement, such as posting a message telling the site’s users that they should try a particular software application that could be used to frustrate copyright enforcement against file sharers. He also provided a link to a torrent file for the recent film *Lord of the Rings: Return of the King* and stated, “if you are curious, download this.” Fung also created a promotional page inviting users to upload torrent files for *Matrix Reloaded*, another recent film. Also “warez” metatags were embedded in the sites for reference by search engines.²⁸⁹⁸

– Defendants and their moderators gave assistance to users engaged in infringement: Fung had personally posted messages in his site’s discussion forum in which he provided technical assistance to users seeking copyrighted works. The sites were also full of statements by moderators who assisted users seeking to download files or provided links to other sites containing the requested infringing items. The court ruled that these moderators, who were under the control of the defendants and had been given authority to moderate the forums and user discussions, were agents of the defendants, and the defendants were therefore responsible for their acts.²⁸⁹⁹

– Defendants implemented technical features promoting copyright infringement: Defendants’ sites allowed users to locate dot-torrent files for desired content, the vast majority of which was infringing. Fung implemented a spider program that located and obtained copies

²⁸⁹⁶ *Id.* at *29-30.

²⁸⁹⁷ *Id.* at *32.

²⁸⁹⁸ *Id.* at *39-43.

²⁸⁹⁹ *Id.* at *44-47.

of dot-torrent files from other sites, including well known infringing sites such as “The Pirate Bay.”²⁹⁰⁰

– Defendants’ business model depended on massive infringing use: The court found there no factual dispute that the availability of copyrighted material was a major draw for users of Fung’s web sites, and there was no dispute that defendants derived revenue from the web site and that this revenue increased along with the number of users.²⁹⁰¹

The court rejected the defendants’ assertions of the safe harbors under Sections 512(a) and 512(d). The court ruled that, as a general proposition, “inducement liability and the Digital Millennium Copyright Act safe harbors are inherently contradictory. Inducement liability is based on active bad faith conduct aimed at promoting infringement; the statutory safe harbors are based on passive good faith conduct aimed at operating a legitimate internet business. Here ... Defendants are liable for inducement. There is no safe harbor for such conduct.”²⁹⁰²

Five months later, the court entered a permanent injunction against the defendants, enjoining them from, among other things, knowingly hosting, indexing, linking to, or otherwise providing access to any Dot-torrent or similar files that correspond, point to or lead to any copyrighted works owned by the plaintiffs and for which the plaintiffs had provided the title to the defendants, on or through any web site, system or software using BitTorrent or any peer-to-peer or other file-sharing or content delivery technology. The defendants were also enjoined from providing technical assistance or support services to users engaged in infringement; maintaining lists of “top” downloads that include the plaintiff’s copyrighted works; including in metadata for any web pages, or maintaining browseable web site categories of Dot-torrent or similar files using, titles of the plaintiffs’ copyrighted works or terms widely known to be associated with copyright infringement (such as “warez,” “Axxo,” “Jaybo,” “DVD Rips,” and the like); or soliciting or targeting a user base generally understood, in substantial part, to be engaging in infringement of or seeking to infringe the plaintiffs’ copyrighted works.²⁹⁰³ The injunction also provided that, “In the event a commercial vendor or other third party becomes able to provide Defendants with a reliable list of Plaintiffs’ Copyrighted Works, Plaintiffs may apply to the Court for an order modifying this Permanent Injunction to relieve them of the obligation of providing Defendants with lists of titles, even if there is a cost to Defendants of securing the lists of titles from the commercial vendor or third party.”²⁹⁰⁴

The Ninth Circuit’s Decision

²⁹⁰⁰ Id. at *51.

²⁹⁰¹ Id. at *55.

²⁹⁰² Id. at *67-68.

²⁹⁰³ Columbia Pictures Industries, Inc. v. Fung, 2010 U.S. Dist. LEXIS 91169 at *20-23 (C.D. Cal. May 20, 2010), rev’d as to scope of injunction, 710 F.3d 1020 (9th Cir. 2013).

²⁹⁰⁴ Id. at *25.

On appeal, the Ninth Circuit affirmed liability on the part of the defendants for inducement. After an extensive recap of the Supreme Court’s Grokster decision, the Ninth Circuit summarized that the inducement principle enunciated in Grokster has four elements: (1) the distribution of a device or product, (2) acts of infringement, (3) an object of promoting its use to infringe copyright, and (4) causation.²⁹⁰⁵ The Ninth Circuit addressed the applicability of each of these elements in turn to the facts of the case.

With respect to element (1) – the distribution of a device or product – Fung argued that because he did not develop or distribute any “device” – that is, the software or technology used for downloading – he was not liable under the inducement principle enunciated in Grokster. The Ninth Circuit disagreed, noting that language in the Supreme Court’s Grokster opinion indicated that inducement liability is not limited to those who distribute a “device,” but also those who provide some service used in accomplishing the infringement.²⁹⁰⁶

With respect to element (2) – acts of infringement – the court began by observing that both uploading and downloading copyrighted material are infringing acts. The former violates the copyright holder’s right to distribution, the latter the right to reproduction. Based on statistical sampling, one of the plaintiffs’ experts averred that between 90 and 96% of the content associated with the torrent files available on Fung’s web sites were for confirmed or highly likely copyright infringing material. Thus, wide acts of infringement were occurring on Fung’s web sites.²⁹⁰⁷

With respect to element (3) – an object of promoting use to infringe copyright – Fung argued that this factor includes two separate elements, the improper object and clear expression or other affirmative steps taken to foster infringement. The court disagreed, ruling that “clear expression or affirmative steps” is not a separate requirement, but rather, an explanation of how the improper object must be proved. The court accordingly concluded that Grokster requires a high degree of proof of the improper object. The improper object must be plain and must be affirmatively communicated through words or actions. Here, there was ample evidence of clear expression or other affirmative steps of unlawful intent, the most important being Fung’s active encouragement of the uploading of torrent files concerning copyrighted content. For a time, one of Fung’s sites, IsoHunt, prominently featured a list of “Box Office Movies,” containing the 20 highest-grossing movies then playing in U.S. theaters. When a user clicked on a listed title, the user would be invited to upload a torrent file for that movie. Fung also posted numerous messages to the IsoHunt forum requesting that users upload torrents for specific copyrighted films; in other posts, he provided links to torrent files for copyrighted movies, urging users to download them. In addition, he responded personally to numerous queries for assistance in uploading torrent files corresponding to obviously copyrighted material, finding particular

²⁹⁰⁵ Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1032 (9th Cir. 2013).

²⁹⁰⁶ Id. at 1033.

²⁹⁰⁷ Id. at 1034.

copyrighted movies and television shows, getting pirated material to play properly, and burning the infringing content onto DVDs for playback on televisions.²⁹⁰⁸

Two types of evidence, insufficient in themselves, corroborated the conclusion that Fung acted with a purpose to cause copyright violations by the use of his services. First, he took no steps to develop filtering tools or other mechanisms to diminish the infringing activity by those using his services. Second, he generated revenue almost exclusively by selling advertising space on his web sites. Because the extent of use of the services determined the gain to Fung, the commercial sense of his business turned on high-volume use, which the record showed was infringing.²⁹⁰⁹

With respect to element (4) – causation – the parties argued competing positions. Fung and amicus curiae Google argued that the acts of infringement must be caused by the manifestations of the distributor’s improper object – that is, by the inducing messages themselves. The plaintiffs argued for a low standard of causation, insisting that they need prove only that the acts of infringement by third parties were caused by the product distributed or services provided. The court adopted the low standard of causation argued by the plaintiffs, ruling that if one provides a service that could be used to infringe copyrights, with the manifested intent that the service actually be used in that manner, that person is liable for the infringement that occurs through the use of the service.²⁹¹⁰

The court went on, however, to state that it was mindful of the potential severity of a loose causation theory for inducement liability. Under this theory of liability, the only causation requirement is that the product or service at issue was used to infringe the plaintiff’s copyrights. The court noted that the possible reach of liability is enormous, particularly in the digital age, and it was therefore important that it not permit inducement liability’s relatively lax causation requirement to enlarge the scope of copyright to encompass control over an article of commerce, such as technology capable of substantial non-infringing uses. The court noted the following limitations flowing out of the Grokster case. Mere knowledge of infringing potential or of actual infringing uses does not subject a product distributor or service provider to liability. When dealing with corporate or entity defendants, the relevant intent must be that of the entity itself, as defined by traditional agency law principles; liability cannot be premised on stray or unauthorized statements that cannot fairly be imputed to the entity. In addition, if an entity begins providing a service with infringing potential at time A, but does not appreciate that potential until later and so does not develop and exhibit the requisite intent to support inducement liability until time B, it would not be held liable for the infringement occurring between times A and B. Relatedly, an individual or entity’s unlawful objective at time B would

²⁹⁰⁸ Id. at 1035-36. In a footnote the court noted that it was not relying on the generic organizational structure of Fung’s web sites – i.e., that they organized files in browsable categories or used an automated indexing program that matched filenames with specific terms. The court said that those features did not themselves send the type of inducing message that would be adequate to prove an unlawful intent. Id. at 1036 n.13.

²⁹⁰⁹ Id. at 1036.

²⁹¹⁰ Id. at 1037.

not be a virus that infects all future actions.²⁹¹¹ “People, companies, and technologies must be allowed to rehabilitate, so to speak, through actions actively discouraging the infringing use of the product, lest the public be deprived of the useful good or service they are still capable of producing.”²⁹¹²

Fung argued that, because other individuals and entities provided services identical to those he offered, causation, even in the relatively loose sense the court had articulated, could not be assumed. He argued that if a user obtained a torrent from a source other than his web sites, he could not be held liable for the infringement that resulted. The court rejected this argument, noting that Fung’s services encompassed more than the provision of torrent files. His trackers managed traffic for torrent files, obtained from his own sites as well as other torrent sites, which enabled users to download copyrighted content. If the plaintiffs could show a sufficient causal connection between users’ infringing activity and the use of Fung’s trackers, the fact that torrent files were obtained from elsewhere could not relieve Fung of liability. The court noted that it need not decide the degree to which Fung could be held liable for having caused infringements by users of his sites or trackers. The only issue presently before the court was the permanent injunction, which did not in this case depend on the exact calculation of infringing use as a basis for a claim of damages. Thus, Fung’s causation arguments were left to the district court to consider when calculating damages. Accordingly, the Ninth Circuit affirmed the district court’s grant of summary judgment to the plaintiffs on the issue of Fung’s liability for inducement.²⁹¹³

After the Ninth Circuit’s decision, Fung agreed to a \$110 million judgment and to shut down his web site by Oct. 23, 2013.²⁹¹⁴

(d) Arista Records v. Lime Group

In Arista Records LLC v. Lime Group LLC,²⁹¹⁵ the defendants distributed the peer-to-peer software client known as LimeWire that enabled users to share digital files across the Gnutella network. The LimeWire client contained a search function in its user interface that enabled the entry of search criteria. LimeWire would then scan the computers of other LimeWire users to locate files matching the search criteria, which could then be downloaded to the searching user’s computer. The plaintiffs, owners of copyrights in various sound recordings that were shared

²⁹¹¹ Id. at 1037-38.

²⁹¹² Id. at 1038.

²⁹¹³ Id. at 1038-39.

²⁹¹⁴ “Website at Center of Copyright Infringement Action Agrees to Shut Down World Wide,” *BNA’s Patent, Trademark & Copyright Journal* (Oct. 17, 2013), available as of Oct. 17, 2013 at http://iplaw.bna.com/iprc/display/simple_doc_display.adp?fedfid=37305808&vname=ptdbulallissuesdib&jd=a0e2n9r2f6&split=0#a0e2n9r2f6.

²⁹¹⁵ 784 F. Supp. 2d 298 (S.D.N.Y. 2011). This opinion amended and replaced a prior opinion issued by the court, reported at 715 F. Supp. 2d 481 (S.D.N.Y. 2010).

without authorization by LimeWire users, brought claims of inducement, contributory infringement, and vicarious infringement against the defendants.²⁹¹⁶

With respect to the claim of inducement, the court granted summary judgment to the plaintiffs. The court noted that under the Supreme Court's Grokster case, inducement constitutes a distinct cause of action from contributory infringement, and requires a showing that the defendant engaged in purposeful conduct that encouraged copyright infringement with the intent to encourage such infringement. The court found purposeful conduct to encourage infringement in the form of distribution of the LimeWire client, which users employed to commit a substantial amount of infringement.²⁹¹⁷

The court found intent on the part of the defendants to encourage infringement from a combination of five factors taken together:

- The defendants' awareness of substantial infringement by LimeWire users: The plaintiffs submitted an expert report showing that LimeWire was overwhelmingly used for infringement. In particular, the expert estimated that 98.8% of the files requested for download through LimeWire were copyright protected or highly likely copyright protected, which made it nearly certain that most actual downloads involved unauthorized content. Internal memoranda at LimeWire regularly discussed the fact that LimeWire users downloaded copyrighted recordings.²⁹¹⁸ For example, a 2001 draft of an offering memorandum in connection with a financing stated that LimeWire "allows people to exchange copyrighted mp3 files" and a 2002 statement of the company's goals acknowledged that, "Currently, the most common use of the Gnutella Network is the sharing of music files, many of them copyrighted."²⁹¹⁹ In 2006, LimeWire developed a strategic plan to "convert" LimeWire users who were sharing unauthorized digital recordings into customers of LimeWire's online music store, which would sell authorized music. In the conversion plan, LimeWire openly acknowledged that the majority

²⁹¹⁶ 784 F. Supp. 2d at 409, 410-11.

²⁹¹⁷ Id. at 424-26. The court found the evidence clearly established direct infringement on the part of LimeWire users, since it demonstrated through documentation and electronic storage media that LimeWire users employed LimeWire to share and download the plaintiffs' copyrighted recordings without authorization. In one interesting side ruling, the court held that a genuine issue of material fact existed as to whether hash-based analysis could independently support a finding of direct infringement. The plaintiffs' expert argued that if two files have the same hash, they are identical, and if two users possess a file with identical hashes, one user's file is a copy of the other. The defendants' expert disputed this conclusion. He agreed that the fact that two users have a file with the same hash implies that the two users possess a file with likely the same content, but it does not imply that those two users shared the file with each other, or that one copied the file from the other. He argued that there are many different ways that the two users could have ended up with the same, identical file, such as by obtaining the file from the same, non-peer-to-peer source such as a web site, or from some non-gnutella-peer-to-peer network, or from some non-LimeWire Gnutella peer. Id. at 424 n.21.

²⁹¹⁸ Id. at 411-12, 426.

²⁹¹⁹ Id. at 426.

of LimeWire's users were infringers. In addition, LimeWire employees maintained a file of articles labeled "Knowledge of Infringement."²⁹²⁰

– The defendants' efforts to attract infringing users: Following Napster's demise, LimeWire announced that it expected 30% to 100% of Napster users to switch to using LimeWire and similar programs such as Kazaa and Morpheus. LimeWire developed plans to attract Napster users to LimeWire, including conducting a marketing campaign through Google AdWords that would direct searches for "Napster" and similar terms to LimeWire. LimeWire also marketed LimeWire as similar to the popular Napster service.²⁹²¹

– The defendants' efforts to enable and assist users to commit infringement: The LimeWire client user interface allowed searching for specific artists or albums, and a number of LimeWire's genre categories, such as "Classic Rock," "SoundTrack," and "Top 40," inevitably guided users to copyrighted recordings. LimeWire employees specifically tested and sought to improve LimeWire's ability to search for and download unauthorized copies of popular copyrighted songs and recordings. And several online communications between LimeWire employees and users specifically assisted LimeWire users in committing infringement.²⁹²²

– The defendants' dependence on infringement for success of its business: LimeWire's sources of revenue (selling advertising space on the LimeWire client and website, and distribution of software bundled with LimeWire) depended on LimeWire attracting the massive user population generated by its infringement-enabling features, and those revenues increased in proportion to the expansion of its user base. Thus, LimeWire's commercial success was derived largely from the high-volume use of LimeWire, most of which was infringing.²⁹²³

– LimeWire's failure to mitigate infringing activities: "The evidence reveals that [the defendants have] not implemented in a meaningful way any of the technological barriers and design choices that are available to diminish infringement through file-sharing programs, such as hash-based filtering, acoustic fingerprinting, filtering based on other digital metadata, and aggressive user education."²⁹²⁴ The court noted that in May 2006, LimeWire had implemented an optional hash-based content filter but that the default setting in the client for the filter was "off." The court noted that LimeWire could have made the hash-based content filter mandatory for all LimeWire users or made the default setting "on." The court further noted that LimeWire had considered, but failed to implement, several other plans to block the availability of infringing content through LimeWire, including a hybrid filtering system that would have combined hash-based filtering and acoustic fingerprinting. The company also developed, but did not implement, its conversion plan, which would have included a user education campaign designed to inform

²⁹²⁰ *Id.* at 426-27.

²⁹²¹ *Id.* at 427-28.

²⁹²² *Id.* at 428-29.

²⁹²³ *Id.* at 429.

²⁹²⁴ *Id.* at 429.

users about the legal consequences of copyright infringement and to promote the purchase of authorized music through the LimeWire online store. Under the conversion plan, LimeWire eventually would have implemented hash-based filtering and acoustic fingerprinting to prevent users from downloading unauthorized files. In addition, LimeWire used keyword-based filtering to allow users to limit their receipt of adult content and active filtering technology to prevent LimeWire users from sharing digital recordings purchased from the LimeWire online store, but did not use any of the filtering technology to screen out copyrighted content from the file-sharing activities of its users. The court found that this selective filtering further demonstrated LimeWire's knowledge of infringement-mitigating technologies and its intentional decision not to employ them in a way that meaningfully deterred its users' infringing activities.²⁹²⁵ "Failure to utilize existing technology to create meaningful barriers against infringement is a strong indicator of intent to foster infringement."²⁹²⁶

Accordingly, the court granted the plaintiffs summary judgment on their claim of inducement of infringement.²⁹²⁷

The court, however, denied the plaintiffs' request for summary judgment with respect to their contributory infringement claim. Although the court found that LimeWire was aware of the prevalence of its users' infringing activities and made a material contribution to that infringement by designing, distributing, supporting, and maintaining the software, the court found material issues of fact as to whether the software was capable of substantial non-infringing uses under the Sony case. In particular, LimeWire had presented evidence of some types of non-infringing content that users share and download through LimeWire in the form of electronic copies of books in the public domain or authorize for distribution, historical documents, archival films and other public domain works, and digital music recordings produced by musicians seeking to promote their work through free online distribution. The court found the record before it insufficient to permit it to assess the technological feasibility or commercial viability of LimeWire's potential non-infringing uses.²⁹²⁸

The court granted the plaintiffs' request for summary judgment with respect to their vicarious liability infringement claim. The court found substantial evidence that LimeWire had the right and ability to limit the use of its product for infringing purposes, including by

²⁹²⁵ Id. at 429-31. The court discounted LimeWire's only step to address infringement – the posting of an electronic notice that appeared when a user first downloaded the LimeWire client, stating that the software was for sharing authorized files only and that downloading the software did not constitute a license for obtaining or distributing unauthorized content. Id. at 431. The user was also required to choose, prior to download, from the following statements: (1) "I will not use LimeWire for copyright infringement." Or (2) I might use LimeWire for copyright infringement." Id. If the user selected the second option, LimeWire would not be downloaded. The court ruled that the notice and statement of intent requirements did not, on their own, constitute meaningful efforts to mitigate infringement. Id.

²⁹²⁶ Id.

²⁹²⁷ Id.

²⁹²⁸ Id. at 433-34.

implementing filtering, denying access and supervising regulating users. The court found that LimeWire possessed a direct financial interest in the infringing activity of its users because LimeWire profited from its ability to attract infringing users, including through increased advertising revenue and increased sales of authorized music and an upgraded version of the LimeWire client that users paid for. The court rejected LimeWire's contention that because LimeWire was capable of substantial non-infringing uses, LimeWire could not be liable for vicarious infringement. The court found no case in which the Sony defense had been applied to a claim of vicarious infringement liability.²⁹²⁹

On Oct. 27, 2010, the court entered a stipulated permanent injunction that, among other things, enjoined LimeWire from copying, reproducing, downloading, distributing, or making available for distribution (by placing in a computer file or folder accessible by others for downloading) any of the plaintiffs' copyrighted works, and from displaying the source code for the LimeWire client. LimeWire was required to use its best efforts to use all reasonable technological means to prevent and inhibit future infringement of the plaintiff's copyrighted works by disabling the searching, downloading, uploading, file trading and file distribution functionality of legacy versions of the LimeWire client software, establishing default settings in the legacy versions that blocked the sharing of unauthorized media titles, and providing all users with a tool to uninstall the legacy versions. Before distributing any new version of the LimeWire client, LimeWire was required to obtain the approval to do so from the plaintiffs and the court.²⁹³⁰ New versions of the client were required to incorporate a "Copyright Filter," which was defined as a "robust and secure means to exhaustively prevent" users from copying, downloading, distributing or communicating to the public the plaintiff's copyrighted works.²⁹³¹ The Copyright Filter was required to include the ability to filter both by text (i.e. artist and song title) and by the use of "Fingerprinting Technology," defined to mean "the most effective available means of content-recognition filtering based on recognizing the unique content of an underlying audio-visual work and detecting and preventing copying of that content no matter how the file containing the content was created (e.g. whether the file was ripped from a CD, DVD, or recorded from a radio or television, etc.), and which is available from commercial vendors such as Audible Magic."²⁹³²

On Mar. 10, 2011, the court issued a ruling with respect to statutory damages to which the plaintiffs were entitled.²⁹³³ The plaintiffs argued that, because the defendants had been found liable for inducing individuals to infringe their copyrights, they should be entitled to recover a separate statutory award for each individual's infringement of a work as to which they were jointly and severally liable. The court rejected this argument and ruled that the plaintiffs were entitled to only one statutory damage award per work from the defendants, regardless of

²⁹²⁹ Id. at 435-36.

²⁹³⁰ Arista Records LLC v. Lime Wire LLC, 2010 U.S. Dist. LEXIS 115675 at *21-24 (S.D.N.Y. Oct. 27, 2010).

²⁹³¹ Id. at *20, *23.

²⁹³² Id. at *20-21.

²⁹³³ Arista Records LLC v. Lime Group LLC, 784 F. Supp. 2d 313 (S.D.N.Y. 2011).

the number of direct infringers of that work with whom the defendants were jointly and severally liable.²⁹³⁴

Section 504(c)(1) allows the recovery of a statutory damages award “for all infringements involved in the action, with respect to any one work, for which any one infringer is liable individually, or for which any two or more infringers are liable jointly and severally.” The plaintiffs argued that the defendants and each direct infringer represented one unit of infringers who were jointly and severally liable, and they should therefore get an award for each such unit. The plaintiffs pointed to a similar hypothetical in Professor Nimmer’s treatise arguing for such an outcome. The court, after a review of relevant precedent, rejected the Nimmer hypothetical and concluded that Congress intended for the copyright statute to treat jointly and severally liable infringers the same way that the statute treats individually liable infringers – just as a plaintiff is entitled to one statutory damage award per work for any individually liable infringer, a plaintiff is entitled to one statutory damage award per work for any two or more jointly and severally liable infringers. The court found that, in situations involving mass infringements, plaintiffs’ position would lead to an absurd result of statutory damages exceeding a billion dollars. And the court noted that the number of direct infringers the defendants induced to infringe could be taken into account in setting the dollar amount of each statutory damage award per work infringed.²⁹³⁵

On April 4, 2011, the court issued a ruling that both an album and a sound recording that the plaintiffs issued as an individual track could constitute a “work” infringed for purposes of computing statutory damages. Specifically, the plaintiffs could recover a statutory damages award for each sound recording that (1) plaintiffs made available as an individual track and (2) that was infringed on the Lime Wire system during the time period in which it was issued as an individual track. However, for those sound recordings that plaintiffs issued only as part of an album, the plaintiffs could recover only one statutory damage award for that album, not for each individual sound recording.²⁹³⁶

In additional follow-up rulings on damages, the court rejected the plaintiffs’ attempt to convert their election from statutory damages to actual damages with respect to untimely registered recordings, as the defendants would be unduly prejudiced by that change one month before trial, particularly in view of the fact that the defendants had been denied certain discovery on the ground that the plaintiffs were seeking only statutory damages.²⁹³⁷ The court also precluded expert testimony showing that other illegal services would have induced infringement of the plaintiffs’ copyrights if the defendants had not done so. The court held that the defendants could not argue they were not responsible for the infringement that took place

²⁹³⁴ *Id.* at 315, 321.

²⁹³⁵ *Id.* at 316-320.

²⁹³⁶ *Arista Records LLS v. Lime Group LLC*, 2011 U.S. Dist. LEXIS 36536 at *7, *18 (S.D.N.Y. Apr. 4, 2011). “Thus, for sound recordings that, like those of the Beatles, we’re apparently not available as individual tracks from iTunes or other services during the time period relevant to this action, Plaintiffs can recover only one award per album infringed.” *Id.* at *18 n.7.

²⁹³⁷ *Arista Records LLC v. Lime Group LLC*, 2011 U.S. Dist. LEXIS 38949 at *8, *10-11 (S.D.N.Y. Apr. 11, 2011).

through the Lime Wire system because that same infringement could have taken place through another system.²⁹³⁸

(e) Flava Works v. Gunter

The facts of this case are set forth in Section III.C.1(b) above. The court dismissed the plaintiff's claim for inducement of copyright infringement because it found that the plaintiff had failed to plead the requirements for an inducement claim as set forth in the Supreme Court's Grokster case. "Plaintiff pleads merely a formulaic recitation of inducement but not facts that plausibly suggest that it is entitled to relief on this theory. It is not enough to allege that myVidster provides storage for video files and encourages sharing (or even that it also knew that the website could be used to infringe). No clear expression of an infringing purpose is alleged, and no active steps taken to foster infringement, such as advertising an infringing use or instructing how to engage in an infringing use, are alleged."²⁹³⁹

(f) Disney Enterprises v. Hotfile

The facts of this case are set forth in Section III.C.6(b)(1)(iii).y below. In adjudicating the plaintiffs' motion for summary judgment with respect to inducement liability under Grokster, the court first surveyed existing authority and noted the following two observations: (1) that, for the most part, recent decisions have suggested that the Sony rule may be raised as a theory of defense where the intent to infringe or induce infringement is not explicit, but rather is imputed from a defendant's material contribution to infringement; and (2) Grokster does not foreclose other common law principles of imputing intent – in particular, a provider may face liability where it knows of particular instances of infringement, rather than simply that the system is capable of infringement or generally permits some level of infringement, and fails to act to remove it.²⁹⁴⁰ Against the body of jurisprudence it had surveyed, the court then summarized the following applicable legal principles for adjudicating claims of inducement and contributory liability against Hotfile (noting uncertainty about whether Grokster introduced a new category of liability based on inducement or whether it spoke to preexisting notions of contributory liability):

[I]t is evident that a defendant will be liable for actually expressing an intention to foster infringement. If that intent is express or can otherwise be said to be "unmistakeable," the *Sony/Betamax* defense will not apply and the defendant will be liable for all acts of direct infringement committed using its systems, as was the case in *Grokster*. Similarly, as explained in *Amazon.com*, where traditional principles permit a court to impute intent

²⁹³⁸ Arista Records LLC v. Lime Group LLC, 785 F. Supp. 2d 423, 425 & 4272 (S.D.N.Y. 2011). "The Court emphasizes that this Order does not preclude the admission of evidence regarding other illegal services for all purposes. Such evidence may be admissible to show (1) that a diminution in Plaintiffs' profits over time is only partially attributable to Defendants (because others caused some of Plaintiffs' actual losses), and (2) the extent to which a large award in this case is likely to deter other infringers." *Id.* at 426.

²⁹³⁹ Flava Works, Inc. v. Gunter, 2011 U.S. Dist. LEXIS 50067 at *17-18 (N.D. Ill. May 20, 2011), rev'd on other grounds, 689 F.3d 754 (7th Cir. 2012).

²⁹⁴⁰ Disney Enterprises, Inc. v. Hotfile Corp., 2013 U.S. Dist. LEXIS 172339 at *105-110.

– for instance, where the defendant knows of specific infringing content available on its system yet fails to remove it – that defendant may be liable, by operation of law, just as if he had actually intended to infringe under *Grokster*. Finally, contributory infringement may be found based on a material contribution theory in instances where a defendant did not express an intention to foster infringement but provided the means for infringement or distributed a commercial product that was subsequently used to infringe. Under that theory, the *Sony/Betamax* rule provides a backstop to liability, immunizing a defendant who demonstrates that noninfringing uses of the system are substantial.²⁹⁴¹

Applying these principles to the facts at hand, the court noted that eight million DMCA notices had been received by Hotfile, and that uploads of those users subject to three or more notices constituted 44 percent of all files on Hotfile and half of all downloaded files in February 2011. At the very least, such activity showed that a high number of Hotfile users likely engaged in infringement, and that the vast majority of Hotfile’s top affiliates and well over 20,000 of its users were likely responsible for a substantial amount of infringement. The plaintiffs had identified over 900,000 files containing their own works that were available for the taking. Before the instant litigation, Hotfile had been sued or threatened with suit by copyright holders, and documents produced in discovery suggested that Hotfile was aware it was becoming “the flagship of non-licensed content,” that if it had examined the files on its system it would have known of the infringing activity, and that it was doing business with those it suspected were infringers, including some of its affiliates. There was also some evidence suggestive of a deliberate design to facilitate infringement, in that its incentive structure rewarded large and frequent file downloads, it paid members through its affiliate program, and it relied on the popularity of content to drive growth, including imploring users to post “interesting” links and media files. Hotfile also provided technical assistance to those who infringed, both by answering specific questions from users about downloading media and by providing tutorials that referenced copyrighted works. Nor, until the complaint was filed, did it take any meaningful action to curtail infringement.²⁹⁴²

In Hotfile’s favor, the court noted that it did not promote any of its files or enable a file search function, so that all infringing activity took place between uploading users, downloading users, and its affiliates. In addition, its system had noninfringing uses, such as the distribution of unlicensed materials. And Hotfile eventually developed a notice and takedown system and, over time, implemented technology to combat infringing users. No document in the record showed a business plan contemplating infringing uses or an understanding that Hotfile was actually assisting users to commit infringement, and no Hotfile employee had posted the plaintiffs’ copyrighted content.²⁹⁴³

The court noted that Hotfile’s general knowledge of infringement, even if rampant, was insufficient by itself to support liability. And unlike *Grokster*, the intent to infringe was not

²⁹⁴¹ *Id.* at *113-14.

²⁹⁴² *Id.* at *115-118.

²⁹⁴³ *Id.* at *118-19.

“unmistakeable” such that it could be said to be central to the business model and ingrained in the platform’s design. Although some evidence showed that Hotfile might have been on notice that specific acts of infringement were afoot, the evidence did not demonstrate that Hotfile knew for certain that the uses were illegal or that Hotfile induced the infringing use. On balance, the court concluded that a number of questions remained regarding Hotfile’s intent (actual or imputed) to foster infringement and the capacity for and scope of noninfringing uses of its system, therefore making summary judgment for inducement or contributory liability inappropriate.²⁹⁴⁴

In Dec. 2013, the MPAA announced a settlement under which the district court had awarded damages of \$80 million to the plaintiffs and ordered Hotfile to either shut down its operations or use digital fingerprinting technology to prevent copyright infringement by its users.²⁹⁴⁵

(g) UMG Recording v. Escape Media

(For a discussion of inducement liability issues in this case, see Section III.C.1(d) above.)

5. Adequacy of Pleadings of Secondary Liability Against Service Providers

A number of cases have addressed the adequacy of pleadings of secondary liability on the part of service providers in view of the principles of liability articulated in the cases in the preceding three subsections.

(a) Miller v. Facebook

In Miller v. Facebook, Inc.,²⁹⁴⁶ the plaintiff, owner of copyright in a video game called “Boomshine” sought to hold Yeo, the developer of another game called “ChainRxn,” directly liable for infringing the look and feel of Boomshine, and to hold Facebook indirectly liable for listing ChainRXn in the Facebook Application Directory and providing the platform through which ChainRXn was distributed. Facebook sought to deny the plaintiff leave to file a second amended complaint. The court granted leave, finding that the proposed second amended complaint adequately pled claims of direct infringement against Yeo and contributory infringement against Facebook.²⁹⁴⁷

With respect to Yeo, the complaint adequately alleged direct infringement of the distribution right by alleging that Yeo published ChainRxn to a publicly accessible web site where it was then distributed to members of the public. It was reasonable to infer that ChainRxn was

²⁹⁴⁴ Id. at *119-23.

²⁹⁴⁵ “Hotfile To Pay \$80M to MPAA, Studios In Copyright Suit,” *Law360* (Dec. 3, 2013), available as of Dec. 7, 2013 at http://www.law360.com/ip/articles/493076?nl_pk=be5fde4e-8dc1-4d81-b621-f0352bcdff74&utm_source=newsletter&utm_medium=email&utm_campaign=ip.

²⁹⁴⁶ 2010 U.S. Dist. LEXIS 61715 (N.D. Cal. May 28, 2010).

²⁹⁴⁷ Id. at *1-3.

downloaded from the computer where it was hosted to the local cache memory of any Facebook user who played the video game. The plaintiff had also adequately pled a violation of the public performance right by Yeo because the video displays of Boomshine could be seen as being publicly performed when users played Yeo's allegedly infringing game.²⁹⁴⁸

Given adequate allegations of direct infringement by Yeo, the court ruled that the plaintiff had also adequately pled contributory infringement against Facebook. Noting that under the Ninth Circuit's decision in Perfect 10 v. Amazon, a computer system operator can be contributorily liable if it has actual knowledge that specific infringing material is available using its system and it could take simple measures to prevent further damage to the copyrighted works, the court ruled that the plaintiff had adequately pled "simple measures" that Facebook could have taken in the form of either disabling Yeo's Facebook account or removing ChainRxn from the Facebook Applications Directory.²⁹⁴⁹

(b) Williams v. Scribd

In Williams v. Scribd, Inc.,²⁹⁵⁰ the court rejected Scribd's arguments why the plaintiff's amended complaint failed to state a claim for contributory and vicarious liability. The plaintiff alleged that a Scribd member uploaded onto the Scribd web site hundreds of pages of his copyrighted material. Noting that under the Ninth Circuit's decision in Napster,²⁹⁵¹ in the online context a plaintiff must allege and show actual knowledge on the part of a service provider for contributory liability, the court found that the plaintiff had adequately pled actual knowledge on the part of Scribd by pleading that he had notified Scribd of the infringement and asked that his materials be removed from the web site. And the plaintiff had adequately pled a material contribution to the infringement both by pleading the mere failure to remove and that the web site provided the site and facilities for direct infringement.²⁹⁵²

The court also rejected Scribd's argument that the plaintiff could not state a claim for vicarious copyright liability because he could not plausibly claim that Scribd benefited financially from the alleged infringement. The court noted that financial benefit exists where the availability of infringing materials acts as a draw for customers, and that the draw need not be substantial. Scribd argued that it had too many works on the site for the copyrighted materials of Williams to be a draw.²⁹⁵³ Citing the Ellison case, the court held "that if the presence of infringing material on Scribd's website compels more people to visit the website than otherwise

²⁹⁴⁸ Id. at *13-15. However, in a confusing aspect of the opinion, the court ruled that the plaintiff had not adequately pled a direct violation of the public display right because the plaintiff's copyright appears to be limited to the source code rather than the audiovisual aspects of the Boomshine, and the source code had not been publicly displayed. Id. at *13.

²⁹⁴⁹ Id. at *20-21.

²⁹⁵⁰ 2010 U.S. Dist. LEXIS 90496 (S.D. Cal. June 23, 2010).

²⁹⁵¹ A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1021 (9th Cir. 2001).

²⁹⁵² Scribd, 2010 U.S. Dist. LEXIS 90496 at *19-20.

²⁹⁵³ Id. at *23-24.

would, thereby making it more attractive to advertisers, Scribd can be said to benefit from the infringement.”²⁹⁵⁴ The court found that the plaintiff had alleged that the misuse of his copyrighted works attracted more users to Scribd’s web site, and that was adequate at the pleading stage – although the court noted that during discovery, Scribd might be able to show that it didn’t in fact generate ad revenues directly or even tangentially from the works of the plaintiff that were uploaded to its site.²⁹⁵⁵

(c) *ALS Scan v. Cloudflare*

In this case, the plaintiff owned a library of copyrighted works of adult entertainment. The plaintiff alleged that defendant Steadfast Networks LLC, a network service provider, hosted pirate sites, including Imagebam.com, that contained unauthorized copies of the plaintiff’s works. Plaintiff alleged that it sent numerous notifications to Steadfast alerting it of infringing content on Imagebam, but Steadfast had failed to remove Imagebam from its servers. The plaintiff asserted claims of contributory and vicarious liability and Steadfast filed a motion to dismiss.²⁹⁵⁶

The court noted that contributory copyright infringement could be imposed under Grokster for intentionally encouraging infringement through specific activity, or under the traditional Gershwin formulation, for having knowledge of the infringing activity, and inducing, causing or materially contributing to the infringing conduct of another. Under relevant Ninth Circuit authority, one can be liable for materially contributing to infringement only where its participation in the infringing conduct of the primary infringer is substantial. The court found the plaintiff had not adequately pled a claim for contributory infringement under these standards. Here, the only allegations specific to Steadfast were it hosted pirate sites, including Imagebam, and that the plaintiff had sent numerous notifications to Steadfast of infringing content on Imagebam, but Steadfast had failed to implement or enforce a repeat infringer policy by removing Imagebam from its servers. The court ruled that because the complaint failed to allege material contribution or inducement, it need not reach the issue of whether Steadfast had knowledge of the infringement. Although the complaint alleged that Steadfast hosted pirate sites that featured infringing content, it was unclear what services Steadfast provided to Imagebam, what type of infringing activity Imagebam conducted (or even what Imagebam was), or how Steadfast contributed to or facilitated that infringement. Because the court was unaware of any authority holding that merely alleging a defendant provided some form of hosting service to an infringing website was sufficient to establish contributory infringement, the court concluded the complaint failed to allege facts establishing that Steadfast materially contributed to infringement.²⁹⁵⁷

²⁹⁵⁴ Id. at *24.

²⁹⁵⁵ Id. at *24-25.

²⁹⁵⁶ ALS Scan, Inc. v. Cloudflare, Inc., 2017 U.S. Dist. LEXIS 46937 at *2-5 (C.D. Cal. Feb. 16, 2017).

²⁹⁵⁷ Id. at *6-14.

The court similarly concluded the complaint failed to adequately plead a claim for inducement because it did not allege that Steadfast provided its services for the purpose of promoting copyright infringement, or that it had directly encouraged Imagebam to display infringing content on its web site. The court also found the complaint failed to adequately plead a claim for vicarious liability because it contained no allegations that Steadfast had a direct financial interest in the infringing activity or had the right and ability to stop the infringing conduct. Because the plaintiff had not adequately pled its primary claims, the court decided it need not address Steadfast's alternative basis for dismissal under the DMCA safe harbors.²⁹⁵⁸

(d) Warner Records v. Charter Communications

Several record labels brought claims for vicarious infringement against Charter Communications based on the use of BitTorrent by Charter's Internet service subscribers to engage in file sharing of the plaintiffs' copyrighted music. A magistrate judge recommended that Charter's motion to dismiss the vicarious liability claims be dismissed based on the following allegations by the plaintiffs: that Charter attracted customers in part by advertising its blazing-fast speeds that allow users to download just about anything instantly, including up to 8 songs in 3 seconds; that the plaintiffs and others had submitted to Charter statutory infringement notices detailing specific infringements committed by specific subscribers, identified by their unique IP addresses but Charter had not taken any steps to address the reported infringements; and that this lack of action likely acted as a draw to further subscriptions, as subscribers knew they could download infringing content without consequence.²⁹⁵⁹

The district court rejected objections raised by Charter to the magistrate judge's articulation of the relevant standard for direct financial benefit and his finding that the plaintiffs had met the standard. With respect to the standard, Charter challenged the magistrate's conclusion that ability to engage in infringing conduct need not be the primary draw of Charter's services, but only *a* draw. Charter interpreted the Ninth Circuit's Perfect 10 v. Giganews decision and other cases as holding that the ability to infringe on the plaintiffs' content must constitute *the* attracting factor for subscribers – pointing to the language in Perfect 10 that infringing activity must be more than an added benefit to a subscription. The court found that Perfect 10 did not support Charter's argument that if infringement is not *the* attracting factor, then it is simply an added benefit. The court found instead that Perfect 10 supported the plaintiffs' position because these plaintiffs, unlike those in Perfect 10, had alleged their works in particular served as a draw. Moreover, the court elaborated that Perfect 10 had focused on whether the infringing use was merely something that customers valued rather than a draw to subscribe. The court therefore ruled that the infringing use need not be *the* draw for subscribers, but rather only that the plaintiffs' work *in particular* constituted a draw.²⁹⁶⁰

²⁹⁵⁸ Id. at *14-20.

²⁹⁵⁹ Warner Records Inc. v. Charter Communications, Inc., 2020 U.S. Dist. LEXIS 66249 at *5-8 (D. Colo. Apr. 15, 2020).

²⁹⁶⁰ Id. at *10-14.

Charter also argued that it did not receive a financial benefit from infringement because it did not affect Charter's revenues whether a subscriber used the Internet to infringe copyrights or for legitimate purposes. The court rejected the argument, finding that Charter had provided no case law to support the claim that a service provider must receive a larger financial benefit from infringing users than from non-infringing users.²⁹⁶¹

The court then concluded that Charter had raised allegations sufficient to show that the ability to download infringing content served as a draw. The plaintiffs alleged that subscribers were motivated to subscribe by Charter's advertisement of features attractive to those who sought to infringe, such as fast download speeds for just about anything. And they had alleged that Charter's failure to stop or take other action in response to notices of infringement acted as a draw to current and prospective subscribers. The court agreed with the plaintiffs that the volume and popularity of the plaintiffs' copyrighted works, the commonality of infringing downloading, and the frequency that the plaintiffs' works in particular were downloaded allowed for the reasonable inference that at least some of Charter's subscribers were drawn by the ability to infringe on the plaintiff's works.²⁹⁶²

The court also rejected Charter's challenges to the magistrate's finding that the plaintiffs plausibly alleged Charter had the practical ability to supervise or control its subscribers' infringing activities. Although the court noted that Charter might lack the ability to identify and terminate all users who infringe on the plaintiffs' copyrighted materials, it could nevertheless stop and limit infringement of the plaintiffs' works by terminating those users about whom it was notified. And the court distinguished the Ninth Circuit's Perfect 10 v. Amazon case by noting that Charter, unlike Google, could terminate its users' ability to access the Internet through Charter. Google lacked such power. Finally, the court rejected Charter's argument that because it could not stop subscribers from using other forms of Internet access to infringe, it had no ability to supervise or control infringing activity. The Court found that Charter could certainly limit its subscribers' ability to infringe by blocking their access to the Internet through Charter, and that fact was sufficient to allege that Charter had the ability to control infringement. The court therefore concluded that the plaintiffs had stated a claim for vicarious copyright infringement.²⁹⁶³

6. Limitations of Liability of Online Service Providers in the DMCA

From late 1995 through May 1996, OSPs, telecommunications carriers and other distributors of online information, content providers and software companies negotiated intensively to reach a consensus on proposed legislation that would provide various statutory safe harbors with respect to the liability of online providers. The parties were unable to reach agreement for legislation in the 103rd Congress. The debate among the various industry

²⁹⁶¹ Id. at *14-15.

²⁹⁶² Id. at *19-21.

²⁹⁶³ Id. at *21-24.

segments was ignited again in connection with the WIPO copyright treaties in Geneva in December of 1996.

(a) History of the Various Legislative Efforts

A number of bills were then introduced in Congress that would limit the liability of OSPs. The first to be introduced was by Rep. Coble on July 17, 1997 (H.R. 2180). This bill would have exempted OSPs from direct or vicarious copyright liability solely based on the transmission or providing of access to online material, and eliminate any damage remedy for contributory liability, limiting plaintiffs to injunctive relief. The criteria for exemption were that the OSP: (a) not initially place the material online; (b) not generate, select, or alter the content of the material; (c) not determine the recipients of the material; (d) not receive a financial benefit directly attributable to a particular act of infringement; (e) not sponsor, endorse, or advertise the material; and (f) either not know or be aware by notice or other information indicating that the material is infringing, or be prohibited by law from accessing the material.

The second bill to be introduced was S. 1146, which, in addition to the WIPO treaty implementation provisions discussed above, also contained provisions limiting liability of OSPs. S. 1146 adopted a different approach to OSP liability than H.R. 2180. It contained three major provisions. First, it provided blanket exemptions from direct, vicarious or contributory liability for OSPs based on the mere provision of defined electronic communications network services or facilities, or on the transmission of private electronic communications, including voice messaging or electronic mail services or real-time communication formats, including chat rooms, streamed data, or other virtually simultaneous transmissions. Second, it provided exemptions from direct, vicarious or contributory liability for the provision of the following information location tools: a site-linking aid or directly, including a hyperlink or index; a navigational aid, including a search engine or browser; and the tools for the creation of a site-linking aid. Third, it provided immunity from direct, vicarious or contributory liability to OSPs for stored third party content, unless upon receiving notice of infringing material that complied with certain defined standards, the OSP failed expeditiously to remove, disable, or block access to the material to the extent technologically feasible and economically reasonable for the lesser of a period of ten days or receipt of a court order concerning the material.

Hearings were held in Sept. of 1997 on both H.R. 2180 and S. 1146. These hearings revealed lingering conflict between service providers and copyright owners on liability issues. Rep. Goodlatte led continuing negotiations between the content providers and OSPs, and to further a compromise, he and Rep. Coble introduced on Feb. 12, 1998 a substitute for H.R. 2180, entitled the "On-Line Copyright Infringement Liability Limitation Act" (H.R. 3209).

On April 1, 1998, the House Judiciary Committee approved the substance of H.R. 3209, but folded it into the pending WIPO implementation legislation, H.R. 2281. Subsequently, based on continuing negotiations, an agreement was finally reached between service providers and copyright owners with respect to the proper scope of liability for online infringements of copyright. H.R. 2281 was then amended to include this compromise agreement.

Meanwhile, similar actions were taking place in the Senate. The provisions of S. 1121, implementing the WIPO treaty, were combined with a new title embodying the compromise agreement between service providers and copyright owners with respect to liability.²⁹⁶⁴ The combined Senate bill was denominated S. 2037, and was unanimously approved by the Senate Judiciary Committee in April of 1998 and adopted by the full Senate in May of 1998.

Both H.R. 2281 and S. 2037 contained the same substantive provisions with respect to OSP liability, which were ultimately adopted in the DMCA.

(b) The OSP Liability Provisions of the DMCA

The liability provisions are contained in Title II of the DMCA. Title II seeks to clearly define the conditions under which an OSP's liability for infringements that occur on the OSP's systems or networks will be limited. Specifically, Title II defines four safe harbors that are codified in a new Section 512 of Title 17. If the OSP falls within these safe harbors, the OSP is exempt from monetary damages and is subject only to carefully prescribed injunctive remedies. As the legislative history states, "New Section 512's limitations on liability are based on functions, and each limitation is intended to describe a separate and distinct function. ... [T]he determination of whether a service provider qualifies for one liability limitation has no effect on the determination of whether it qualifies for a separate and distinct liability limitation under another new subsection of new Section 512."²⁹⁶⁵ This principle was codified in Section 512(n) of the DMCA, which provides: "Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection."²⁹⁶⁶

Under Section 512(i) establishes a condition for eligibility for all the safe harbors. Specifically, they will apply only if the service provider "(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and (B) accommodates and does not interfere with standard technical measures."²⁹⁶⁷ The term "standard technical measures" is defined as "technical measures that are used by copyright owners to identify or protect copyrighted works and – (A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process; (B) are available to any person on reasonable and

²⁹⁶⁴ Sen. Patrick Leahy and Sen. John Ashcroft drafted the compromise agreement for incorporation into pending legislation.

²⁹⁶⁵ H.R. Rep. No. 105-551 Part 2, at 65 (1998).

²⁹⁶⁶ 17 U.S.C. § 512(n).

²⁹⁶⁷ 17 U.S.C. § 512(i)(1)(A) & (B).

nondiscriminatory terms; and (C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.”²⁹⁶⁸

(1) Safe Harbors – Definition of a “Service Provider”

The four safe harbors are described below and are applicable to a “Service Provider.” Under Section 512(k), for purposes of the first safe harbor, a “Service Provider” is defined as “an entity offering the transmission, routing or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received.” For purposes of the other three safe harbors, a “Service Provider” is defined more broadly to be “a provider of online services or network access, or the operator of facilities therefor.” The latter definition would seem to cover a broad array of OSPs, BBS operators, system operators, search engines, portals, and the like. It is also probably broad enough to cover the owners and operators of corporate intranets, university networks and interactive websites.²⁹⁶⁹

In Marvel Enterprises, Inc. v. NCSoft Corp.,²⁹⁷⁰ the court dismissed the plaintiffs’ claim in their complaint for declaratory judgment that the defendants did not qualify as a “service provider” under the DMCA safe harbors and thus would not be protected from liability thereunder. The court noted the rule that a plaintiff may not seek declaratory relief as an advance ruling on a potential affirmative defense. From their allegations, it was clear that the plaintiffs were seeking a determination of the defendants’ ability to use the DMCA as a defense. Because the issues on which the plaintiffs sought declaratory judgment related only to the defendants’ liability for the remainder of the plaintiffs’ claims, the declaratory judgment would not independently resolve the controversy between the parties, but rather would merely determine a collateral legal issue governing certain aspects of the dispute. The court concluded that the plaintiffs were therefore inappropriately seeking an advance ruling on a potential affirmative defense.²⁹⁷¹

(i) Acting as a Mere Conduit for Infringing Information – Section 512(a)

The first safe harbor is essentially a codification of the Netcom case and a rejection of the Frena case, at least to the extent that the Frena case suggested that passive, automatic acts

²⁹⁶⁸ 17 U.S.C. § 512(i)(2)(A), (B) & (C).

²⁹⁶⁹ Ian C. Ballon & Keith M. Kupferschmid, “Third Party Liability under the Digital Millennium Copyright Act: New Liability Limitations and More Litigations for ISPs,” *Cyberspace Lawyer*, Oct. 1998, at 3, 4. The legislative history states that the definition “includes universities and schools to the extent they perform the functions identified in” the definition. H.R. Rep. No. 105-551 Part 2, at 64 (1998).

²⁹⁷⁰ 2005 U.S. Dist. LEXIS 8448 (C.D. Cal. Mar. 9, 2005).

²⁹⁷¹ *Id.* at *18-19.

engaged in through a technological process initiated by another through the facilities of an OSP could constitute direct infringement on the part of the OSP.²⁹⁷²

Specifically, under Section 512(a), a Service Provider is not liable for monetary relief, and is subject only to limited injunctive relief, for “transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if:

(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

(5) the material is transmitted through the system or network without modification of its content.”

This safe harbor will not be available to a Service Provider that initiates, selects, or modifies the content of a transmission, or stores it on a system in a way that its content becomes generally accessible to third parties.

The safe harbor of Section 512(a) has been tested in the following cases:

a. The Napster Case

In the Napster case, discussed extensively in Section III.C.2.(c)(1) above, Napster moved for summary judgment that it was immune from the plaintiffs’ claims by virtue of the Section 512(a) safe harbor. Napster argued that it fell within the subject matter of the safe harbor because its “core function” was to offer the “transmission, routing, or providing of connections for digital online communications” by enabling the connection of users’ hard-drives and the

²⁹⁷² H.R. Rep. No. 105-551 Part 1, at 11 (1998); ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619, 622 (4th Cir. 2001). “Subsections (a)(1) through (5) limit the range of activities that qualify under this subsection to ones in which a service provider plays the role of a ‘conduit’ for the communications of others.” H.R. Rep. No. 105-551 Part 2, at 51 (1998).

transmission of MP3 files “directly from the Host hard drive and Napster browser through the Internet to the user’s Napster browser and hard drive.”²⁹⁷³ Napster argued that it satisfied the preceding five specific conditions for the safe harbor because “(1) a Napster user, and never Napster itself, initiates the transmission of MP3 files; (2) the transmission occurs through an automatic, technical process without any editorial input from Napster; (3) Napster does not choose the recipients of the MP3 files; (4) Napster does not make a copy of the material during transmission; and (5) the content of the material is not modified during transmission.”²⁹⁷⁴

The court rejected the applicability of the Section 512(a) safe harbor to Napster for several reasons. First, the court held that the safe harbor could not provide a complete defense to Napster’s entire system because the system performed more than just the functions of transmission, routing, and providing of connections. Specifically, the court noted that Section 512(n) of the DMCA provides that the four safe harbors “describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsections.”²⁹⁷⁵ The court ruled that the Napster system, through its index of user files and its “hot list” feature that each functioned as an “information location tool,” undisputedly performed some information location functions which, if those functions were to be immunized, must satisfy the separate provisions of the safe harbor set forth in Section 512(d) (discussed in subsection (iv) below).²⁹⁷⁶

Napster argued that, even if its system functioned in part as an information location tool, that function should be considered incidental to the system’s core function of transmitting MP3 music files, and the safe harbor of Section 512(a) should therefore provide a complete defense to its system. The court rejected this argument, holding that because the parties disputed material issues regarding the operation of Napster’s index, directory and search engine, the court could not hold for purposes of summary judgment that the information location tool aspects of the Napster system were peripheral to the alleged infringement, or that they should not be analyzed separately under Section 512(d).²⁹⁷⁷

The court then rejected the applicability of Section 512(a) to Napster for two principal reasons. First, the court noted that the preamble of Section 512(a) makes the safe harbor applicable only to service providers “transmitting, routing or providing connections for, material through a system or network controlled or operated by or for the service provider” (emphasis added). The court found it undisputed that MP3 files do not pass “through” Napster’s servers,

²⁹⁷³ A&M Records Inc. v. Napster, Inc., 54 U.S.P.Q.2d 1746, 1749 (N.D. Cal. 2000), aff’d in part & rev’d in part on other grounds, 239 F.3d 1004 (9th Cir. 2001).

²⁹⁷⁴ Id.

²⁹⁷⁵ 17 U.S.C. § 512(n).

²⁹⁷⁶ Napster, 54 U.S.P.Q.2d at 1750.

²⁹⁷⁷ Id. at 1750.

but rather “through” the Internet, and ruled that the Internet could not be considered “a system or network controlled or operated by or for the service provider.”²⁹⁷⁸ The court rejected Napster’s argument that its system should be deemed to include the Napster browser on its users’ computers and that the MP3 files were transmitted “through” that browser: “[E]ven if each user’s Napster browser is part of the system, the transmission goes from one part of the system to another, or between parts of the system, but not ‘through’ the system. The court finds that subsection 512(a) does not protect the transmission of MP3 files.”²⁹⁷⁹

Second, the court called into question whether Napster had complied with the prefatory conditions of Section 512(i) of the DMCA (discussed further in subsection (2) below), which imposes additional requirements on eligibility for any DMCA safe harbor. Section 512(i) requires that the Service Provider adopt and reasonably implement, and inform subscribers and account holders of the Service Provider’s system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the Service Provider’s system or network who are repeat infringers.

The court found questions about Napster’s compliance with Section 512(i) on two grounds. The first ground was that, although Napster claimed to have had an oral policy from the earliest days of its existence, Napster had not adopted a *written* policy for termination of repeat infringers until after the litigation was filed. The court noted that, even were the written policy ultimately adopted an adequate one, the late adoption of a formal written policy would not necessarily moot the plaintiffs’ claims to monetary relief for past harms.²⁹⁸⁰ The second ground was that the court believed Napster had not established that it *reasonably* implemented a policy for terminating repeat infringers. Specifically, the court noted that Napster blocked users about whom it received notices of infringement by blocking that user’s password, but not the Internet Protocol (IP) address of the user. (The parties sharply disputed whether it would be feasible or effective to block IP addresses.) The court further noted the plaintiffs’ argument that, because Napster did not maintain the actual identity of its users (their real names and physical addresses), blocked users could readily reapply for a new account on the Napster system and continue their infringing activity. The court therefore concluded that the plaintiffs had raised genuine issues of material fact about whether Napster had reasonably implemented a policy of

²⁹⁷⁸ *Id.* at 1751.

²⁹⁷⁹ *Id.* (emphasis in original). The court similarly found that the Napster system did not provide *connections* “through” its system. “Although the Napster server conveys address information to establish a connection between the requesting and host users, the connection itself occurs through the Internet. ... Drawing inferences in the light most favorable to the non-moving party, this court cannot say that Napster serves as a conduit for the connection itself, as opposed to the address information that makes the connection possible. Napster enables or facilitates the initiation of connections, but these connections do not pass through the system within the meaning of subsection 512(a).” *Id.* at 1752.

²⁹⁸⁰ *Id.* at 1753.

terminating repeat infringers, and therefore denied Napster's motion for summary judgment based on a Section 512(a) defense.²⁹⁸¹

b. Ellison v. Robertson

In Ellison v. Robertson,²⁹⁸² an individual named Robertson scanned several fictional works written by the plaintiff and posted them onto the Usenet group "alt.binaries.e-book," a group that was used primarily to exchange pirated and unauthorized digital copies of text material, principally works of fiction by famous authors. AOL, acting as a Usenet peer, hosted the infringing materials on its Usenet server for a period of fourteen days. The plaintiff sought to hold AOL liable for direct, vicarious and contributory copyright infringement.²⁹⁸³ AOL asserted that the plaintiff could not establish the elements for common law liability and that it was immune under the Section 512(a) and Section 512(c) safe harbors of the DMCA. The district court, relying on the Netcom case, ruled that AOL could not be liable for direct copyright infringement merely based on its passive role as a provider of Usenet services.²⁹⁸⁴ The court's rulings with respect to contributory infringement are discussed in Section III.C.2(e) above.

With respect to vicarious liability, the plaintiff argued that, under the Ninth Circuit's Napster I decision, AOL's ability to block infringers' access to its Usenet servers was sufficient to establish the right and ability to control infringing activity. The court rejected this argument, noting the same Catch 22 under the Section 512(c) safe harbor this would set up that the court noted in the Hendrickson v. eBay case: Because an OSP is required under Section 512(c)(1)(C) to delete or block access to infringing material, if this ability to delete or block were sufficient to establish the "right and ability to control" infringing activity, the OSP would thereby be disqualified from the safe harbor under Section 512(c)(1)(B), at least if it received a financial benefit directly attributable to the infringing activity.²⁹⁸⁵ "The Court does not accept that Congress would express [an intention that ISPs which receive a financial benefit directly attributable to the infringing activity could not qualify for the Section 512(c) safe harbor under any circumstance] by creating a confusing, self-contradictory catch-22 situation that pits 512(c)(1)(B) and 512(c)(1)(C) directly at odds with one another, particularly when there is a much simpler explanation: the DMCA requires more than the mere ability to delete and block access to infringing material after that material has been posted in order for the ISP to be said to have 'the right and ability to control such activity.'"²⁹⁸⁶

The court further found that AOL's right and ability to control the infringing behavior was substantially less than that enjoyed by the OSP in the Netcom case, where the OSP was one of

²⁹⁸¹ Id.

²⁹⁸² 189 F. Supp. 2d 1059 (C.D. Cal. 2002).

²⁹⁸³ Id. at 1053-54.

²⁹⁸⁴ Id. at 1056.

²⁹⁸⁵ Id. at 1060-61.

²⁹⁸⁶ Id. at 1061.

two entities responsible for providing the direct infringer with access to the Internet. As a result, by taking affirmative steps against the other entity, the OSP had the ability to target the infringer himself and deny him access to the Internet. By contrast, AOL had no such ability to go after the individual who had posted the infringing copies of the plaintiff's works onto Usenet. The court therefore concluded that AOL's ability to delete or block access to the infringing postings after they had found their way onto AOL's Usenet servers was insufficient to constitute the right and ability to control the infringing activity for purposes of common law vicarious liability.²⁹⁸⁷

With respect to the financial benefit prong of vicarious liability, the district court held that AOL received no direct financial benefit from the infringing activity. The court ruled that the direct financial benefit prong requires a showing that a "substantial" proportion of a defendant's income be directly linked to infringing activity.²⁹⁸⁸ AOL did not receive any financial compensation from its peering agreements and participation in Usenet, and the availability of Usenet did not act as a "draw" for customers under the Napster I case. In particular, the court noted that any "draw" to a particular newsgroup, such as alt.binaries.e-book, was miniscule, as the pro rata "draw" of a single newsgroup was only about 0.00000596% of AOL's total usage (there were 43,000 total newsgroups available through AOL). Usenet usage constituted a very small percentage of total AOL usage, and the plaintiff had not produced any evidence that a significant portion of even that minimal usage entailed the illegal exchange of copyrighted material.²⁹⁸⁹ Accordingly, the court granted summary judgment to AOL on the plaintiff's claim for vicarious liability.²⁹⁹⁰

On appeal, the Ninth Circuit affirmed the finding of no vicarious liability, although the Ninth Circuit disagreed with the district court's ruling that to establish a direct financial benefit, the plaintiff must show that a "substantial" proportion of a defendant's income be directly linked to infringing activity. The Ninth Circuit stated that it is sufficient if infringing activity is a "draw" for customers, and there is no requirement that such draw be "substantial."²⁹⁹¹ "The essential aspect of the 'direct financial benefit' inquiry is whether there is a causal relationship between the infringing activity and any financial benefit a defendant reaps, regardless of *how substantial* the benefit is in proportion to a defendant's overall profits."²⁹⁹²

The Ninth Circuit ruled that the plaintiff had not submitted sufficient evidence to raise a triable issue of fact under the direct financial benefit prong, and in the course of its discussion, fleshed out what sort of evidence would be required to show that infringing activity on a particular site constitutes a "draw" to that site:

²⁹⁸⁷ Id. at 1061-62.

²⁹⁸⁸ Id. at 1062-64.

²⁹⁸⁹ Id. at 1062-63.

²⁹⁹⁰ Id. at 1064.

²⁹⁹¹ Ellison v. Robertson, 357 F.3d 1072, 1078-79 (9th Cir. 2004).

²⁹⁹² Id. at 1079 (emphasis in original).

We recognize, of course, that there is usually substantial overlap between aspects of goods or services that customers value and aspects of goods or services that ultimately draw the customers. There are, however, cases in which customers value a service that does not “act as a draw.” Accordingly, Congress cautions courts that “receiving a one-time set-up fee and flat periodic payments for service ... [ordinarily] would not constitute receiving a ‘financial benefit directly attributable to the infringing activity.’” S. Rep. 105-190, at 44. But “where the value of the service lies in providing access to infringing material,” courts might find such “one-time set-up and flat periodic” fees to constitute a direct financial benefit. *Id.* at 44-45. Thus, the central question of the “direct financial benefit” inquiry in this case is whether the infringing activity constitutes a draw for subscribers, not just an added benefit.²⁹⁹³

The Ninth Circuit found that there was no evidence that AOL customers either subscribed because of the available infringing material or canceled subscriptions because it was no longer available. Accordingly, no jury could reasonably conclude that AOL received a direct financial benefit from providing access to the infringing material, and the claim for vicarious liability failed.²⁹⁹⁴

The district court also ruled on an assertion by AOL of two of the DMCA safe harbors – the Section 512(a) and the Section 512(c) safe harbors. The district court noted that as a predicate for any of the safe harbors, AOL had to satisfy the requirement of Section 512(i) that it have adopted and reasonably implemented, and informed its subscribers, of a policy for the termination in appropriate circumstances of subscribers who are repeat infringers.²⁹⁹⁵ Citing the legislative history, the court ruled that Section 512(i) does not require OSPs to take affirmative steps to investigate potential infringement and set up notification procedures in an attempt to identify the responsible individuals committing infringement through the system. Rather, it was sufficient to satisfy Section 512(i) that AOL’s terms of service, to which every AOL member had to agree, included a notice that AOL members could not make unauthorized copies of content protected by intellectual property rights and their accounts could be terminated for making such unauthorized copies.²⁹⁹⁶

The plaintiff challenged whether AOL had reasonably implemented its termination policy by noting that no subscriber had ever been terminated from AOL as a repeat infringer and AOL had not at the time of the infringement defined how many times a user had to be guilty of infringement before being classified as a repeat infringer. The court rejected this challenge, noting that Section 512(i) does not require AOL to actually terminate repeat infringers or even to

²⁹⁹³ *Id.*

²⁹⁹⁴ *Id.*

²⁹⁹⁵ The court noted that such a policy must have been adopted, reasonably implemented and noticed to subscribers at the time the allegedly infringing activity occurred. “Doing so after the infringing activity has already occurred is insufficient if the ISP seeks a limitation of liability in connection with that infringing activity.” Ellison v. Robertson, 189 F. Supp. 2d 1059, 1064 (C.D. Cal. 2002).

²⁹⁹⁶ *Id.* at 1064-65.

investigate infringement in order to determine if AOL users are behind it. “That is the province of subsection (c), which provides detailed requirements related to notification of infringement and the ISPs’ responsibility to investigate and, in some instances, delete or block access to infringing material on their systems. Subsection (i) only requires AOL to put its users on notice that they face a realistic threat of having their Internet access terminated if they repeatedly violate intellectual property rights.”²⁹⁹⁷ The court therefore held that AOL had satisfied the predicate requirements of Section 512(i).²⁹⁹⁸

The district court then turned to application of the Section 512(a) safe harbor. The court first noted that Section 512(a) “does not require ISPs to remove or block access to infringing materials upon receiving notification of infringement, as is the case with subsections (c) and (d).”²⁹⁹⁹ The plaintiff argued that AOL was not engaged in “intermediate and transient storage”³⁰⁰⁰ required under Section 512(a) because it maintained Usenet materials on its server for fourteen days. The court posed the issue under Section 512(a) as follows: “Certain functions such as the provision of e-mail service or Internet connectivity clearly fall under the purview of subsection (a); other functions such as hosting a web site or chatroom fall under the scope of subsection (c). The question presented by this case is which subsection applies to the function performed by AOL when it stores USENET messages in order to provide USENET access to users.”³⁰⁰¹ The court answered that Section 512(a) applies, based primarily on the fact that the legislative history of the Section 512(a) safe harbor expressly noted that the exempted storage and transmissions under that section “would ordinarily include forwarding of customers’ Usenet postings to other Internet sites in accordance with configuration settings that apply to all such postings.”³⁰⁰² The court further ruled that storage of the Usenet postings for fourteen days was

²⁹⁹⁷ *Id.* at 1066. An important implication of this ruling appears to be that an OSP can qualify for the Section 512(a) safe harbor regardless of whether it promptly deletes infringing material or terminates repeat infringers, so long as it has a policy to do so and otherwise complies with the requirements of the Section 512(a) safe harbor. The court further stated: “[T]he ‘realistic threat of losing [Internet] access’ that Congress wishes ISPs to impress upon would-be infringers remains just that – a mere threat – unless the ISP decides to implement procedures aimed at identifying, investigating, and remedying infringement in hopes of meeting the requirements of subsection (c)’s safe harbor. Such an arrangement makes a certain amount of sense. If subsection (i) obligated ISPs to affirmatively seek out information regarding infringement and then investigate, eradicate, and punish infringement on their networks, then most if not all of the notice and takedown requirements of the subsection (c) safe harbor would be indirectly imported and applied to subsections (a) and (b) as well. This would upset the carefully balanced, ‘separate function-separate safe harbor-separate requirements’ architecture of the DMCA.” *Id.* at 1066 n.15.

²⁹⁹⁸ *Id.* at 1066.

²⁹⁹⁹ *Id.* at 1068.

³⁰⁰⁰ Clause (4) of Section 512(a) requires that “no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections.”

³⁰⁰¹ *Id.* at 1068.

³⁰⁰² *Id.* at 1069-70 (quoting H.R. Rep. 105-551(I) at p. 24).

not too long to disqualify the storage as intermediate and transient. The court noted that Usenet messages had been stored for eleven days in the Netcom case, and that three days was an insufficient difference to distinguish the present case from Netcom. Accordingly, the court ruled that AOL's Usenet storage was "intermediate and transient."³⁰⁰³

The court further ruled that AOL had satisfied the remaining requirements of Section 512(a). The transmission of the plaintiff's newsgroup message was not initiated by AOL, AOL did not select the individual postings on the alt.binaries.e-book newsgroup (and the fact that AOL decided not to carry every newsgroup did not constitute selection of the specific material giving rise to the claim of infringement³⁰⁰⁴), AOL did not select the recipients of the material,³⁰⁰⁵ and the material was transmitted through AOL's system without modification of its content.³⁰⁰⁶ Accordingly, the court concluded that AOL qualified for the Section 512(a) safe harbor, and that it therefore needed not reach the issue of whether the Section 512(c) safe harbor also applied.³⁰⁰⁷

On appeal, the Ninth Circuit reversed the ruling that AOL was entitled to the Section 512(a) safe harbor on the ground that there were triable issues of material fact concerning whether AOL had met the threshold requirements of Section 512(i). The Ninth Circuit ruled, however, that if after remand a jury found AOL to be eligible under Section 512(i) to assert the DMCA safe harbors, then "the parties need not relitigate whether AOL qualifies for the limitation of liability provided by § 512(a); the district court's resolution of that issue at the summary judgment stage is sound."³⁰⁰⁸

With respect to Section 512(i), the Ninth Circuit found it difficult to conclude that AOL had reasonably implemented a policy against repeat infringers, because there was ample evidence in the record suggesting that AOL did not have an effective notification procedure in place at the time the alleged infringing activities were taking place. Although AOL had notified the Copyright Office of its correct email address before Ellison's attorney attempted to contact AOL and did post its correct email address on the AOL website with a brief summary of its policy as to repeat infringers, AOL also changed the email address to which infringement notifications were supposed to have been sent and failed to provide for forwarding of messages sent to the old address or notification that the email address was inactive.³⁰⁰⁹ The Ninth Circuit found that

³⁰⁰³ 189 F. Supp. 2d at 1070.

³⁰⁰⁴ To impute selection of the infringing material to the ISP, "the better interpretation of [512](a)(2) is that the ISP would have to choose specific postings, or perhaps block messages sent by users expressing opinions with which the ISP disagrees." Id. at 1071.

³⁰⁰⁵ To impute selection of the recipients of the material to AOL, "the better interpretation is that AOL would have to direct material to certain recipients (e.g. all AOL members whose names start with 'G') but not others." Id.

³⁰⁰⁶ Id. at 1070-72.

³⁰⁰⁷ Id. at 1072 & n.22.

³⁰⁰⁸ Ellison v. Robertson, 357 F.3d 1072, 1074 (9th Cir. 2004).

³⁰⁰⁹ Id. at 1080.

AOL should have closed the old email account or forwarded the emails sent to the old account to the new one. The fact that AOL had allowed notices of potential copyright infringement to go unheeded for a period of time was sufficient for a reasonable jury to conclude that AOL had not reasonably implemented its policy against repeat infringers.³⁰¹⁰

c. The Aimster/Madster Lawsuits

The facts of the Aimster/Madster lawsuits are set forth in Section III.C.2(c)(3) above. In that case, Aimster asserted the Section 512(a) safe harbor (as well as the Section 512(c) safe harbor, discussed in Section III.C.6(b)(1)(iii).e below). In ruling on Aimster's assertions of the safe harbors, the district court first noted that the DMCA safe harbors could potentially apply to liability for direct, vicarious and contributory copyright infringement.³⁰¹¹ Note that this holding is consistent with the Ninth Circuit's holding in Napster I, in which the court ruled that the safe harbors could potentially shield against vicarious liability,³⁰¹² but inconsistent with the CoStar case, which concluded that the safe harbors cannot shield against vicarious liability (see the discussion in Section III.C.6(b)(1)(iii).c below).

The district court then turned to whether Aimster had satisfied the predicate conditions of meeting the definitions of "service provider" in Sections 512(k)(1)(A) & (B) and adopting an adequate policy of termination of repeat infringers under Section 512(i)(1)(A). The court found that Aimster qualified as a "service provider" because a "plain reading of both definitions reveals that 'service provider' is defined so broadly that we have trouble imagining the existence of an online service that *would not* fall under the definitions."³⁰¹³

The district court found, however, that Aimster had not adopted an adequate policy to terminate repeat infringers. Although Aimster's copyright notice on its site informed users of a procedure for notifying Aimster when infringing activity was taking place on the system and stated that users who were found to repeatedly violate copyright rights of others may have their access to all services terminated, the court held that the policy was not reasonably implemented because it in fact *could not* be implemented. In particular, the encryption on Aimster rendered it impossible to ascertain which users were transferring which files, nor did Section 512(i) obligate the plaintiffs to provide the Internet protocol address of a particular copyright infringer on the Aimster system to assist Aimster in implementing its termination policy.³⁰¹⁴ "Adopting a repeat infringer policy and then purposely eviscerating any hope that such a policy could ever be carried

³⁰¹⁰ Id.

³⁰¹¹ In re Aimster Copyright Litigation, 252 F. Supp. 2d 634, 657 (N.D. Ill. 2002).

³⁰¹² The district court's 2002 decision on the plaintiffs' motion for summary judgment in the MP3Board case, discussed in Section III.D.8 below, also at least implicitly recognized that the Section 512(d) safe harbor could apply to a claim of vicarious liability.

³⁰¹³ Id. at 658 (emphasis in original).

³⁰¹⁴ Id. at 659.

out is not an ‘implementation’ as required by § 512(i).”³⁰¹⁵ Accordingly, Aimster’s failure to comply with Section 512(i) rendered it ineligible for any of the safe harbors.³⁰¹⁶

In addition, the court ruled that Aimster had not satisfied the particular conditions for the Section 512(a) safe harbor because, relying on one of the district court’s decisions in the Napster case, the information transferred between individual Aimster users did not pass “through” Aimster’s system at all by virtue of its peer-to-peer architecture (Section 512(a) immunizes liability by virtue of a service provider’s transmitting, routing or providing connections for, “materials through a system or network controlled or operated by or for the service provider”).³⁰¹⁷ The holdings of the Napster and Aimster courts on this point, if adopted by other courts, will make it difficult for the Section 512(a) safe harbor ever to apply to a peer-to-peer architecture. The court rejected Aimster’s argument that “through” should be interpreted to mean “by means of” or “by the help or agency of.”³⁰¹⁸ Finally, the court noted that Aimster was ineligible for the Section 512(a) safe harbor because its encryption of the information transferred between users constituted a modification of that information, which Section 512(a) does not permit.³⁰¹⁹

On appeal, the Seventh Circuit affirmed that Aimster was not entitled to any of the safe harbors of the DMCA, but based its conclusion solely on the ground that Aimster had not complied with the predicate conditions of Section 512(i). “Far from doing anything to discourage repeat infringers of the plaintiffs’ copyrights, Aimster invited them to do so, showed them how they could do so with ease using its system, and by teaching its users how to encrypt their unlawful distribution of copyrighted materials disabled itself from doing anything to prevent infringement.”³⁰²⁰

d. Perfect 10 v. CCBill

The District Court’s Decision

The plaintiff, Perfect10, owner of the copyrights in an extensive collection of pornographic photos, brought a copyright infringement lawsuit against CWIE, an OSP hosting various sites that allegedly contained infringing copies of Perfect10’s photos, as well as several related third parties providing ancillary services to such sites: IBill, a company that processed payments for online merchants, Internet Key, an age verification service for adult content websites, and CCBill, a provider of a fully automated Internet service that enabled consumers to use credit cards or checks to pay for subscriptions or memberships to e-commerce venues

³⁰¹⁵ Id.

³⁰¹⁶ Id.

³⁰¹⁷ Id. at 659-60.

³⁰¹⁸ Id. at 660.

³⁰¹⁹ Id. at 660 n.19.

³⁰²⁰ In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004).

created and offered by CCBill's clients.³⁰²¹ Each of the defendants raised various of the DMCA safe harbors as defenses, of which the Section 512(a) defenses will be discussed here (the remaining defenses are discussed in the subsections below).

Perfect 10 challenged the various defendants' ability to rely on the safe harbors for failure to comply with the predicate requirements of Section 512(i) as well as failure to meet the substantive criteria of the individual safe harbors. The court considered the factual posture of each of the defendants in turn, and the case is particularly interesting because it is the first to comprehensively adjudicate the adequacy of specific language comprising a policy to terminate repeat infringers. The court began its analysis with some general observations about the DMCA, and quoted from the Fourth Circuit's decision in the ALS Scan case that the safe harbor immunity is afforded "only to 'innocent' service providers who can prove they do not have actual or constructive knowledge of the infringement, as defined under any of the three prongs of 17 U.S.C. § 512(c)(1). The DMCA's protection of an innocent service provider disappears at the moment the service provider loses its innocence, i.e., at the moment it becomes aware that a third party is using its system to infringe. At that point, the Act shifts responsibility to the service provider to disable the infringing matter ..."³⁰²²

The court then turned to the applicability of the safe harbors to each of the individual defendants as follows:

IBill. The court first considered the adequacy of IBill's policy to terminate repeat infringers under Section 512(i). Under IBill's policy, when it received a notice of infringement that substantially complied with the DMCA requirements, it suspended payment processing services to that client. If IBill determined that it had received previous complaints about that client or the website, IBill terminated the account permanently. Perfect 10 argued that this policy was inadequate because it suspended services for particular websites without terminating the webmaster responsible for that material. The court rejected this argument, noting that the focus of Section 512(i) is on infringing users rather than on content. The policy of disabling of IBill clients accused of infringing third party copyrights was therefore adequate.³⁰²³

Perfect 10 argued that IBill had not reasonably implemented its termination policy because it had not kept a log of its notifications of infringement. The court held that the DMCA does not require an OSP to keep a log of its notifications. Because IBill had kept the actual DMCA notifications it had received, this was sufficient to demonstrate that it adequately tracked its notifications.³⁰²⁴ The court further held that many of the notifications Perfect 10 had sent to IBill were inadequate to trigger a duty to act on them. Several such notices were emails from Perfect 10's counsel that identified several websites run by IBill's clients that contained allegedly

³⁰²¹ Perfect 10, Inc. v. CCBill, 340 F. Supp. 1077, 1082-84 (C.D. Cal. 2004).

³⁰²² Id. at 1086 (citations omitted).

³⁰²³ Id. at 1088-89.

³⁰²⁴ Id. at 1089.

infringing material, but did not identify the URLs of the infringing images nor identify which of Perfect 10's copyrighted images were being infringed. The court held that the failure to identify the URLs or the copyrighted images made the notices inadequate. Another notice identified the URL of an infringing image, although not the copyrighted work that it allegedly infringed. The court ruled that, although the notice did not comply with all of the requirements of Section 512(c)(3)(a), the supply of a URL was sufficiently substantial compliance to give rise to a duty to act.³⁰²⁵ Because IBill had acted on the single sufficient notice by suspending the account of the website, the court concluded that IBill had reasonably implemented its repeat infringer policy.³⁰²⁶

With respect to the Section 512(a) safe harbor, Perfect 10 argued that IBill did not qualify because it did not transmit the infringing material at issue, but rather only credit card information. In an important holding, the court read the scope of Section 512(a) very expansively to cover IBill based on the language of Section 512(a) that affords immunity for "providing connections for material through a system or network controlled or operated by or for the service provider."³⁰²⁷ The court concluded that IBill was within this language: "IBill provides a connection to the material on its clients' websites through a system which it operates in order to provide its clients with billing services."³⁰²⁸ Accordingly, the court granted summary judgment to IBill under the Section 512(a) safe harbor.³⁰²⁹

Internet Key. Perfect 10 challenged Internet Key's compliance with the threshold requirements of Section 512(i) based on its termination policy, which read as follows:

Banned Webmaster

If a webmaster, identified by either the webmaster's name, vendorID or common ownership entity, has had three (3) websites which have been denied participation in the SexKey program in accordance with this policy, that webmaster will be denied participation in its program of any webmaster or website in its discretion.

...

Repeat Offenders

The participation of any website deemed to be a repeat offender will be terminated.

Banned Websites

Pending receipt of a Counter Notification, participation of the website subject to a Notification will be suspended. A website will be permanently prohibited from

³⁰²⁵ Id. at 1089-90.

³⁰²⁶ Id. at 1090.

³⁰²⁷ Id. at 1091.

³⁰²⁸ Id. The court rejected Perfect 10's reliance on the Aimster case, noting that the Aimster case dealt with the transmission of material, not the provision of a connection to the material. Id. at 1091-92.

³⁰²⁹ Id. at 1092.

participating in the SexKey program upon receipt by the Company of a second Notification.³⁰³⁰

The court ruled that this policy, which provided that Internet Key would disable access to an affiliate website after it received a single notification of an infringement, and would permanently ban a webmaster from Internet Key after it had received three notifications regarding websites of any particular webmaster, was legally adequate.³⁰³¹ “In order for an infringer to be a ‘repeat’ infringer, he or she must infringe at least twice. Therefore, the Court finds that Internet Key’s policy of terminating a webmaster after 3 notifications is reasonable.”³⁰³²

Perfect 10 next challenged Internet Key’s implementation of its termination policy, arguing that it had provided Internet Key with 22,000 pages of printouts from SexKey affiliated web sites which infringed its rights, together with many full-sized printouts of the images that constituted infringement, and Internet Key did not disable access to the infringing web sites. The court found Perfect 10’s notices of infringement inadequate under the DMCA. A letter from Perfect 10’s counsel accompanying the document production failed to identify which documents were found on Internet Key’s affiliate web sites, did not contain a statement that the information in the notification was accurate, and did not state that the author had a good faith belief that the information in the letter was accurate nor was there a declaration under penalty of perjury. Although the letter identified which images were infringing, it did not identify which copyrights of Perfect 10 the images infringed. Perfect 10’s notice was therefore not compliant with the DMCA, and absent a DMCA-compliant notice, the court ruled that Perfect 10 had failed to raise a genuine issue of material fact concerning whether Internet Key met the threshold requirements of Section 512(i).³⁰³³

With respect to the Section 512(a) safe harbor, the court ruled that Internet Key’s age verification service function fell within the functions described in Section 512(a) – specifically, Internet Key was “providing connections for material” on its client web sites through a system it operated to provide its clients with adult verification services. The court therefore granted summary judgment to Internet Key on the Section 512(a) safe harbor for infringement claims arising after the date it adopted its DMCA policy (but denying summary judgment for infringement claims prior to the date Internet Key put a DMCA policy into place).³⁰³⁴

³⁰³⁰ Id. at 1093-94.

³⁰³¹ Id. at 1094.

³⁰³² Id. at 1094 n.12. The court also rejected Perfect 10’s challenge to the reasonableness of Internet Key’s termination policy on the ground that Internet Key’s web site identified one person as its designated copyright agent, whereas Internet Key’s owner testified that its agent was a company. The court rejected this challenge, noting that Internet Key had never failed to respond to notices, and in any event it appeared that Internet Key likely had more than one individual who responded to notifications of copyright infringement. Id. at 1094.

³⁰³³ Id. at 1095-97.

³⁰³⁴ Id. at 1098-99.

CWIE and CCBill. Perfect 10 challenged the repeat infringer policies of CWIE and CCBill under Section 512(i) on a number of grounds. First, it argued that their DMCA notice spreadsheet was missing several webmaster names of its affiliate sites. The court rejected this challenge, noting that only a few webmaster names were missing from the spreadsheet in instances where the notice was deficient or the issues were resolved, and such was insufficient to raise a genuine issue of material fact that CWIE and CCBill did not reasonably implement their repeat infringer policies.³⁰³⁵

Second, Perfect 10 argued that CWIE and CCBill had failed to act in response to a number of infringement notices Perfect 10 had sent. The court found, however, that such notices were deficient under the DMCA because they identified only the web sites containing allegedly infringing material, but did not identify the URLs of the infringing images or which of Perfect 10's copyrights were being infringed.³⁰³⁶

Finally, Perfect 10 argued that it submitted several emails to CWIE regarding password hacking web sites that provided passwords to Perfect 10's web sites and CWIE failed to discontinue hosting those web sites. The court ruled, however, that Perfect 10 had not submitted any evidence that the use of the passwords actually resulted in the infringement of Perfect 10's copyrights. Accordingly, Perfect 10 had failed to raise any genuine issues of material fact that CWIE and CCBill did not reasonably implement their repeat infringer policies.³⁰³⁷

With respect to the applicability of the Section 512(a) safe harbor to CCBill, Perfect 10 argued that CCBill did not fall within that safe harbor because it did not transmit the infringing material at issue. Perfect 10 argued that Section 512(a) provides protection only for OSPs who transmit the allegedly infringing material and not other material, such as credit card information. Once again, however, the court found CCBill entitled to Section 512(a)'s safe harbor because CCBill provided a "connection" to the material on its clients' web sites through a system which it operated in order to provide its clients with billing services. Accordingly, the court granted summary judgment to CCBill under the Section 512(a) safe harbor.³⁰³⁸

The Ninth Circuit's Decision.

Perfect 10 appealed the rulings that CCBill and CWIE qualified for immunity under the Section 512 safe harbors. Turning first to the threshold question of whether CCBill and CWIE had reasonably implemented a policy for termination of repeat infringers, the Ninth Circuit ruled that a service provider "implements" a policy "if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners

³⁰³⁵ Id. at 1099-1100.

³⁰³⁶ Id. at 1100-01.

³⁰³⁷ Id. at 1101.

³⁰³⁸ Id. at 1102-03.

from collecting information needed to issue such notifications.”³⁰³⁹ The court noted that the statute permits service providers to implement a variety of procedures, “but an implementation is reasonable if, under ‘appropriate circumstances,’ the service provider terminates users who repeatedly or blatantly infringe copyright.”³⁰⁴⁰

The Ninth Circuit agreed with the district court’s rejection of Perfect 10’s argument that CCBill and CWIE had prevented the implementation of their policies by failing to keep track of repeatedly infringing webmasters. Citing the Ellison and Aimster cases, the court ruled that, although substantial failure to record webmasters associated with allegedly infringing websites could raise a genuine issue of material fact as to the implementation of the service provider’s repeat infringer policy for purposes of summary judgment, in this case the record did not reflect such a failure. Perfect 10 had submitted a single page from CCBill’s and CWIE’s “DMCA Log” showing some empty fields in the spreadsheet column labeled “Webmasters Name,” and argued that this page showed no effort to track notices of infringements received by webmaster identity. The court noted, however, that the remainder of the DMCA Log indicated that the email address and/or name of the webmaster was routinely recorded in CCBill’s and CWIE’s DMCA Log, and CCBill’s interrogatory responses also contained a chart indicating that CCBill and CWIE largely kept track of the webmaster for each website. Accordingly, the district court had properly concluded that the DMCA Log did not raise a triable issue of fact that CCBill and CWIE did not implement a repeat infringer policy.³⁰⁴¹

With respect to whether CCBill and CWIE had reasonably implemented their repeat infringer policies, the Ninth Circuit first noted that to identify and terminate repeat infringers, a service provider need not affirmatively police its users for evidence of repeat infringement.³⁰⁴² Perfect 10 argued that CCBill’s and CWIE’s implementation of their repeat infringer policies was unreasonable because they had received notices of infringement from Perfect 10, yet the infringement identified in the notices continued. The Ninth Circuit, however, agreed with the district court’s rulings that such notices did not substantially comply with the requirements of Section 512(c)(3). To be substantially compliant, a notice from a copyright holder must substantially comply with all of Section 512(c)(3)’s clauses, not just some of them.³⁰⁴³

Specifically, the court noted that a 22,185 page set of notices including pictures with URLs of Perfect 10 models allegedly posted on CCBill or CWIE client websites did not contain a statement under penalty of perjury that the complaining party was authorized to act, as required by Section 512(c)(3)(A)(vi). Other notices sent by Perfect 10 similarly had one or more of the required elements missing. The court noted that a copyright holder should not be permitted to

³⁰³⁹ Perfect 10, Inc. v. CCBill LLC, 481 F.3d 751, 758 (9th Cir.), cert. denied, 552 U.S. 1062 (2007).

³⁰⁴⁰ Id. at 758-59.

³⁰⁴¹ Id. at 759-60.

³⁰⁴² Id. at 760.

³⁰⁴³ Id. at 760-61.

cobble together adequate notice from separately defective notices.³⁰⁴⁴ “The DMCA notification procedures place the burden of policing copyright infringement – identifying the potentially infringing material and adequately documenting infringement – squarely on the owners of the copyright. We decline to shift a substantial burden from the copyright owner to the provider; Perfect 10’s separate communications are inadequate.”³⁰⁴⁵

The Ninth Circuit disagreed, however, with the district court’s refusal to consider evidence of notices provided by any party other than Perfect 10 on the basis that such notices would be irrelevant to Perfect 10’s claims. The court held that CCBill’s and CWIE’s actions toward copyright holders who were not a party to the litigation would be relevant in determining whether CCBill and CWIE reasonably implemented their repeat infringer policies. Accordingly, the court remanded for determination of whether CCBill and/or CWIE implemented its repeat infringer policy in an unreasonable manner with respect to any copyright holder other than Perfect 10.³⁰⁴⁶

The court next noted that, in importing the knowledge standards of Section 512(c) to the analysis of whether a service provider reasonably implemented its Section 512(i) repeat infringer policy, Congress had also imported the “red flag” test of Section 512(c)(1)(A)(ii). Perfect 10 argued that CCBill and CWIE had failed to reasonably implement their repeat infringer policy because they were aware of a number of red flags that signaled apparent infringement and had failed to act. Specifically, Perfect 10 argued that, because CCBill and CWIE had provided services to “illegal.net” and “stolencelebritypics.com,” they must have been aware of apparent infringing activity.³⁰⁴⁷ The Ninth Circuit disagreed. “When a website traffics in pictures that are titillating by nature, describing photographs as ‘illegal’ or ‘stolen’ may be an attempt to increase their salacious appeal, rather than an admission that the photographs are actually illegal or stolen. We do not place the burden of determining whether photographs are actually illegal on a service provider.”³⁰⁴⁸

The court also rejected Perfect 10’s argument that password-hacking sites hosted by CWIE obviously infringed. The court noted that, in order for a website to qualify as a red flag of infringement, it would need to be apparent that the website instructed or enabled users to infringe another’s copyright.³⁰⁴⁹ “We find that the burden of determining whether passwords on a website enabled infringement is not on the service provider. The website could be a hoax, or out of date. ... There is simply no way for a service provider to conclude that the passwords enabled infringement without trying the passwords, and verifying that they enabled illegal access

³⁰⁴⁴ Id. at 761-62.

³⁰⁴⁵ Id. at 762.

³⁰⁴⁶ Id. at 762-63.

³⁰⁴⁷ Id. at 763.

³⁰⁴⁸ Id.

³⁰⁴⁹ Id.

to copyrighted material. We impose no such investigative duties on services providers. Password hacking websites are thus not *per se* ‘red flags’ of infringement.”³⁰⁵⁰

Perfect 10 argued that CCBill and CWIE had also failed the predicate condition of Section 512(i)(1)(B) of not interfering with standard technical measure used to identify or protect copyrighted works, by blocking Perfect 10’s access to CCBill affiliated websites in order to prevent Perfect 10 from discovering whether those websites infringed Perfect 10’s copyrights. The Ninth Circuit found two disputed facts at issue for purposes of summary judgment. First, the court was unable to determine on the record whether accessing websites is a standard technical measure that was developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process, as required by Section 512(i)(2)(A). Second, even if it were a standard technical measure, CCBill claimed it blocked Perfect 10’s credit card only because Perfect 10 had previously reversed charges for subscriptions. Perfect 10 insisted CCBill did so in order to prevent Perfect 10 from identifying infringing content. If CCBill were correct, Perfect 10’s method of identifying infringement – forcing CCBill to pay the fines and fees associated with chargebacks – might well impose a substantial cost on CCBill. If not, CCBill might well have interfered with Perfect 10’s efforts to police the websites in question for possible infringements. Accordingly, the court remanded to the district court for determinations on whether access to a website is a standard technical measure, and if so, whether CCBill’s refusal to process Perfect 10’s transactions interfered with that measure for identifying infringement.³⁰⁵¹

Finally, the court turned to issues of whether CCBill and CWIE were entitled to the Section 512(a) safe harbor. Agreeing with the district court, the Ninth Circuit rejected Perfect 10’s argument that CCBill was not eligible for immunity under Section 512(a) because it did not itself transmit the infringing material. The court noted that Section 512(a) provides a broad grant of immunity to service providers whose connection with the infringing material is transient. In the course of an Internet transmission of information through multiple computers, all intervening computers provide transient connections among users. The court read Section 512(a) to grant immunity to all service providers for transmitting all online communications, not just those that directly infringe.³⁰⁵²

The court noted that CCBill transmitted credit card information and proof of payment, both of which were digital online communications. However, there was little information in the record as to how CCBill sent the payment it received to its account holders, and it was unclear whether such payment was a digital communication, transmitted without modification to the content of the material, or was transmitted often enough such that CCBill was only a transient holder. Accordingly, on the record before it, the court ruled that it could not conclude that

³⁰⁵⁰ Id. at 763-64.

³⁰⁵¹ Id. at 764.

³⁰⁵² Id. at 765.

CCBill was a service provider under Section 512(a), and remanded to the district court for further consideration of the issue.³⁰⁵³

e. Columbia Pictures v. Fung

In Columbia Pictures Industries, Inc. v. Fung,³⁰⁵⁴ the defendants operated BitTorrent sites through which users could search indexes for dot-torrent files pointing to infringing movies and other content. The district court found the defendants liable for inducement of infringement and rejected assertion of a safe harbor under Section 512(a) – because of the way the BitTorrent protocol worked, infringing materials did not pass through the defendants’ system, which the court ruled was a prerequisite for the Section 512(a) safe harbor.³⁰⁵⁵

On appeal, the Ninth Circuit affirmed, although on a different rationale. It began its analysis with an examination of whether applying the safe harbor to inducement liability would be inconsistent with Section 512(i)(a)(A)’s requirement that the service provider implement a policy of removing repeat infringers. The court concluded that there was no inherent incompatibility. In some instances the Grokster standard of inducement might be met even where a service provider had a policy of removing proven repeat infringers. It was therefore conceivable that a service provider liable for inducement could be entitled to protection under the safe harbors.³⁰⁵⁶ Said the court: “In light of these considerations, we are not clairvoyant enough to be sure that there are no instances in which a defendant otherwise liable for contributor copyright infringement could meet the prerequisites for one or more of the DMCA safe harbors. We therefore think it best to conduct the two inquiries independently – although, as will appear, aspects of the inducing behavior that give rise to liability are relevant to the

³⁰⁵³ Id. The Ninth Circuit also made an important ruling with respect to Section 230 of the Communications Decency Act (CDA), which states that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider,” and expressly preempts any state law to the contrary. 47 U.S.C. §§ 239(c)(1), (e)(3). The immunity created by Section 230(c)(1) is limited by Section 230(e)(2), which requires the court to “construe Section 230(c)(1) in a manner that would neither ‘limit or expand any law pertaining to intellectual property.’” Thus, Section 230 does not clothe service providers in immunity from “law[s] pertaining to intellectual property.” The CDA does not contain an express definition of “intellectual property.” The Ninth Circuit expressed the view that, “[b]ecause material on a website may be viewed across the Internet, and thus in more than one state at a time, permitting the reach of any particular state’s definition of intellectual property to dictate the contours of this federal immunity would be contrary to Congress’s expressed goal of insulating the development of the Internet from the various state-law regimes.” Id. at 768. Accordingly, the Ninth Circuit construed the term “intellectual property” to mean “federal intellectual property,” and concluded that CCBill and CWIE were eligible for CDA immunity “for all of the state claims raised by Perfect 10.” Id. Although the only state intellectual property claims the plaintiff had raised were trademark claims, the Ninth’s Circuit’s seemingly categorical ruling that Section 230’s website immunity preempts all state intellectual property claims would presumably apply to state copyright law claims.

³⁰⁵⁴ 2009 U.S. Dist. LEXIS 122661 (C.D. Cal. Dec. 21, 2009), aff’d, 710 F.3d 1020 (9th Cir. 2013).

³⁰⁵⁵ Id. at *60 n.26.

³⁰⁵⁶ Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1040 (9th Cir. 2013).

operation of some of the DMCA safe harbors and can, in some circumstances, preclude their application.”³⁰⁵⁷

Turning to the applicability of the Section 512(a) safe harbor in particular, the Ninth Circuit noted that the district court was in error to find Fung ineligible for the Section 512(a) safe harbor on the ground that infringing materials were not passing through or residing on Fung’s system. The Ninth Circuit had previously ruled in CCBill that Section 512(a) provides immunity for transmitting all digital online communications, not just those that directly infringe. Here, although it was not clear the plaintiffs were seeking to establish liability based directly on the tracking functions of Fung’s trackers, those trackers generated information concerning the torrent files transmitted that Fung then compiled and used to induce further infringing use of his web sites and trackers. In that sense, the tracking function was connected to the basis on which liability was sought and found (the dot-torrent files Fung collected and indexed). Without determining whether that information-generating use would itself affect the availability of the Section 512(a) safe harbor, the court held the safe harbor not available for Fung’s trackers on other grounds. Specifically, the trackers did not fit the definition of “service provider” applying to the Section 512(a) safe harbor, which requires the service provider to provide connections between or among points *specified by a user*. In this case, it was Fung’s tracker that selected the “points” (i.e., the publishers from which chunks of data would be transmitted) to which a user’s client would connect in order to download a file, not the users themselves. Accordingly, the Section 512(a) safe harbor was not available to Fung.³⁰⁵⁸

After the Ninth Circuit’s decision, Fung agreed to a \$110 million judgment and to shut down his web site by Oct. 23, 2013.³⁰⁵⁹

f. American Broadcasting v. Aereo

The court’s rulings with respect to why Aereo’s Internet retransmissions of copyrighted broadcasts were not entitled to the Section 512(a) safe harbor are discussed in Section II.B.10 above.

g. Rosen v. Global Net Access

The court’s rulings with respect to why Global Net Access was not entitled to the Section 512(a) safe harbor are discussed in Section III.C.2(p) above.

h. BMG v. Cox Communications

³⁰⁵⁷ Id.

³⁰⁵⁸ Id. at 1041.

³⁰⁵⁹ “Website at Center of Copyright Infringement Action Agrees to Shut Down World Wide,” *BNA’s Patent, Trademark & Copyright Journal* (Oct. 17, 2013), available as of Oct. 17, 2013 at http://iplaw.bna.com/iprc/display/simple_doc_display.adp?fedfid=37305808&vname=ptdbulallissuesdib&jd=a0e2n9r2f6&split=0#a0e2n9r2f6.

The Proceedings in the District Court

In BMG Rights Management (US) LLC v. Cox Communications, Inc.,³⁰⁶⁰ the plaintiff BMG Rights Management (“BMG”)³⁰⁶¹ sought to hold the defendants Cox Communications, Inc. and Cox Com, LLC (“Cox”) contributorily and vicariously liable for alleged infringement of BMG’s musical composition copyrights taking place over Cox’s high-speed Internet service by virtue of users’ use of the BitTorrent protocol to illegally upload and download music files. BMG enlisted Rightscorp, Inc. as its agent to identify infringing uses of its copyrighted works. Rightscorp owned software that searched web sites that indexed torrent files and identified files that appeared to contain one or more of BMG’s copyrighted works. As the court noted, a torrent file does not contain any content. It contains metadata about the files available to be distributed via the BitTorrent protocol and other information that allowed Rightscorp’s software to contact a BitTorrent tracker and find peers offering torrent payloads that contained the files. If Rightscorp’s software contacted a peer and determined the peer had the torrent payload, Rightscorp’s software recorded the date, time, the peer’s IP address, the port on the peer’s computer through which the connection was made, the torrent file’s unique hash value, and the name of the copyrighted work. Rightscorp then sent a notice of infringement to the Internet service provider associated with the recorded IP address. BMG alleged that Rightscorp sent Cox 2.5 million notices corresponding to instances in which Cox Internet users offered one of BMG’s copyrighted works for download.³⁰⁶² BMG also contended that Rightscorp’s software downloaded more than 100,000 full copies of music files that violated its musical composition copyrights from peers through Cox’s Internet service. Cox asserted the Section 512(a) safe harbor and BMG brought a motion for summary judgment that Cox was not entitled to the safe harbor as a matter of law, which the court granted.³⁰⁶³

³⁰⁶⁰ 149 F. Supp. 3d 634 (E.D. Va. 2015).

³⁰⁶¹ A second plaintiff, Round Hill Music LP, also brought copyright infringement claims against the defendants, but the court ruled that the pertinent agreements submitted by Round Hill to establish its standing did not give it either co-ownership of the copyrights it asserted in the litigation or an exclusive license for any use of the copyrights, but rather established Round Hill as merely the provider of day-to-day administrative services with respect to the copyrights. The court therefore dismissed Round Hill’s claims for infringement against the defendants. *Id.* at 648-53.

³⁰⁶² *Id.* at 639-40. The 2.5 million number of notices was disputed. Rightscorp asserted that during the time period relevant to the litigation, it issued an infringement notice only when its software confirmed that a peer was offering 100% of its payload. Rightscorp admitted that beginning in December 2014, after the filing of the lawsuit, it began sending notices when a payload contained anywhere between 10% and 100%, as indicated by a bitfield in the torrent file. The court noted that, because a torrent payload may contain hundreds of files, establishing that a peer is offering 10% of a payload is not a guarantee that the work identified in a notice was in fact in the payload. Cox claimed that over 500,000 of the 2.5 million notices were issued after the lawsuit was filed and therefore, for at least some of those notices, the peer did not actually have the allegedly infringing file. Cox also argued that Rightscorp could not establish that it was utilizing a 100% bitfield threshold during the time period relevant to the suit. *Id.* at 640 n.1.

³⁰⁶³ *Id.* at 640, 653 & 662.

The court turned first to whether Cox had a policy to terminate the accounts of users who were repeat infringers, and if so, whether Cox had reasonably implemented that policy, as required by Section 512(i). The court found that Cox did have a policy to terminate repeat infringers. Cox's Acceptable Use Policy ("AUP") stated that account holders could not use Cox's Internet service to post, copy, transmit, or disseminate any content that infringed the copyrights or other intellectual property rights of any party. The AUP further provided that violation of any terms of the AUP could result in the immediate suspension or termination of either access to Cox's Internet service and/or the Cox account. Cox informed its account holders of the policy in subscriber agreements. The terms on Cox's web site also incorporated the AUP by reference.³⁰⁶⁴

Cox implemented the AUP through an abuse department that handled misconduct on its network. Abuses handled ranged from copyright infringement to hacking to excessive bandwidth usage. Cox offered copyright owners an email address, abuse@cox.net, to which they could send notices of infringement. Cox processed the notices it received using a largely automated system called the Cox Abuse Tracking System or CATS. CATS scanned the messages in the inbox and culled certain information, such as the date of the alleged abuse and IP address, then used the information to create a "ticket." Three features of the CATS operations were noted by the court. First, when Cox received multiple complaints in one day for a single account, the tickets were "rolled up," meaning that Cox counted only the first ticket. Second, Cox imposed a "hard limit" on the number of complaints a complainant could submit that would receive customer-facing action. If a complainant exceeded the hard limit, CATS automatically sent an email informing the complainant that the daily limit had been reached and the tickets created from those emails were automatically closed. The default limit was 200 complaints per complainant per day, but Cox was willing to work with a complainant to set a reasonable number. Cox asserted that such limits were necessary to keep the number of complaints at a manageable capacity for staff and to prevent a single complainant from overwhelming the company. Third, Cox defined its "abuse cycle" in 180-day periods. While Cox maintained a record of its customers' full ticket histories, if no complaints were received within six months from the last complaint, the cycle restarted.³⁰⁶⁵

Cox handled tickets generated by CATS according to its "graduated response procedure." This procedure, which Cox did not publicize to customers, progressed from warnings to suspensions and, ultimately, the possibility of termination. Cox took no action on an account's first ticket because a substantial percentage of accounts never received a second complaint within one abuse cycle. When a second complaint arrived, CATS generated an email to the account holder that included a letter from Cox explaining the alleged infringement as well as the complete text of the infringement notice Cox received from the copyright owner. When Cox had "rolled up" complaints over the course of a day, CATS would send only the first complaint received that day. This process of sending an email warning repeated on the third, fourth, fifth, sixth and seventh complaints Cox received for an account within a six-month period. When Cox received an eighth notice, it suspended the account and placed the account holder in what Cox

³⁰⁶⁴ *Id.* at 640.

³⁰⁶⁵ *Id.* at 640-41.

called a “soft-walled garden,” in which the account holder’s Internet access was temporarily limited to a single web page that displayed a warning message. The account holder could exit the soft-walled garden and self-reactivate service by clicking a link on the web page. On the ninth complaint, the account holder was again sent to the soft-walled garden.³⁰⁶⁶

The tenth complaint resulted in what Cox called a “hard-walled garden,” in which the account holder was directed to a web page with instructions to call Cox customer service. When the account holder called, he or she could request reactivation. The eleventh complaint produced the same result. The twelfth and thirteenth complaints also placed account holders in the hard-walled garden, but required them to speak to higher-level Cox customer service representatives to request reactivation. When Cox received the fourteenth complaint in an abuse cycle, it reviewed the full account history and considered termination. Termination was never automatic, however, and was left to the discretion of Cox employees. Cox asserted that in the vast majority of cases, it was able to address the behavior triggering the infringement notices during the preliminary steps and never had to reach the drastic measure of terminating service.³⁰⁶⁷

Rightscorp included within its standard infringement notice an offer of settlement. Specifically, the notices said, “This notice is an offer of settlement. If you click on the link below and login to the Rightscorp, Inc. automated settlement system, for \$10.00 [or \$20.00] per infringement, you will receive a legal release from the copyright owner.”³⁰⁶⁸ As a policy, Cox did not accept or process infringement notices that contained settlement offers. Cox’s in-house counsel set the policy after concluding that such notices were improper and fell outside the “spirit” of the DMCA. When Cox received a complaint with a settlement offer, it asked the complainant to conform the notice to Cox’s policy and explained that the notice would not be forwarded unless and until it was amended. Until a complainant complied, Cox “blacklisted” all complaints received from that complainant by configuring CATS to auto-delete messages received from that complainant’s email address.³⁰⁶⁹

On Mar. 9, 2011, Cox received its first notice of infringement from Rightscorp. Cox asked Rightscorp to remove its settlement offers, but Rightscorp declined to do so and continued to send Cox notices. On Mar. 14, Cox blacklisted Rightscorp, so that from that point on Cox auto-deleted Rightscorp’s emails and never retrieved the information from the body of those notices. Cox asserted that the following October Rightscorp started inundating its inbox, sending as many as 24,000 notices in one day. In response, Cox blocked Rightscorp’s messages entirely, so that they would never even enter Cox’s inbox. Thus, while blacklisting a complainant still resulted in

³⁰⁶⁶ Id. at 641.

³⁰⁶⁷ Id. at 641-42.

³⁰⁶⁸ Id. at * 642.

³⁰⁶⁹ Id.

Cox maintaining a record of the emails received and deleted, blocking a complainant (as Cox did to Rightscorp) results in no record of any message received.³⁰⁷⁰

The parties disputed what Section 512(i) means for a service provider to “reasonably implement” a repeat infringer termination policy. The district court noted that courts have interpreted the phrase to impose two separate requirements: (1) that a service provider *implemented* its policy, and (2) that implementation was reasonable. With respect to the first requirement, the court noted that under existing case law, the service provider must have a working notification system and a procedure for dealing with DMCA-compliant notifications, and the provider must not actively prevent copyright owners from collecting information needed to issue such notifications. Additionally, the penalty imposed for repeat infringers (when appropriate circumstances exist) must be termination and not some lesser consequence.³⁰⁷¹

With respect to the second requirement, a service provider’s implementation is reasonable if it terminates a repeat infringer’s access in appropriate circumstances. The court noted that two questions are pertinent to such termination – when should a service provider consider a subscriber or account holder to be a repeat infringer, and when do circumstances become appropriate for termination. The court rejected Cox’s suggestion that one can be labeled an infringer only when adjudicated by a court as such, finding no support in the case law for that interpretation. Rather, the court observed that courts had articulated a knowledge standard – a policy is unreasonable if the service provider failed to respond when it had knowledge of the infringement. But even if a service provider has knowledge of infringement, Section 512(i) requires termination only in “appropriate circumstances.” Based on court decisions and the legislative history, the court concluded that appropriate circumstances cover, at a minimum, instances where a service provider is given sufficient evidence to create actual knowledge of blatant, repeat infringement by particular users, particularly infringement of a willful and commercial nature.³⁰⁷²

The court then applied this standard to the facts of the case. BMG argued that Cox did not reasonably implement its repeat infringer policy for three reasons. First, it argued that Cox had not implemented its policy at all since it refused to accept Rightscorp’s infringement notices merely because they contained settlement offers, and it was unreasonable to make no effort to record the date and time of the infringing activity and the account holder’s IP address contained in such notices. Second, BMG argued that with millions of subscribers, Cox’s use of a hard limit on the number of infringement notices it would receive in a twenty-four-hour period was unreasonable. Third, BMG argued that Cox did not terminate access of repeat infringers under appropriate circumstances.³⁰⁷³

³⁰⁷⁰ Id.

³⁰⁷¹ Id. at 653-54.

³⁰⁷² Id. at 654-55.

³⁰⁷³ Id. at 655.

The court found the last of these three asserted grounds sufficient, standing alone, to bar Cox from invoking the Section 512(a) safe harbor. Accordingly, the court found no need to decide whether Cox's refusal to receive notices with settlement agreements or its hard limit on the number of notices received might also render Cox ineligible for a safe harbor. The court also noted that Because Cox was not acting on or receiving Rightscorp's notices, its analysis would focus on how Cox treated notices of infringement received from copyright owners other than BMG. In assessing Cox's termination of repeat infringers, the court divided Cox's practices into two time periods: before the fall of 2012 and after.³⁰⁷⁴

Turning first to the time period before the fall of 2012, the court found the record conclusively established that during that period Cox did not implement its repeat infringer policy at all. Instead, the court found that Cox publicly purported to comply with its policy, while privately disparaging and intentionally circumventing the DMCA's requirements. According to the court, Cox employees followed an unwritten policy put in place by senior members of Cox's abuse group by which accounts used to repeatedly infringe copyrights would be nominally terminated, only to be reactivated upon request. Once these accounts were reactivated, customers were given clean slates, meaning the next notice of infringement Cox received linked to those accounts would be considered the first in Cox's graduated response procedure. The court found that numerous emails in the record supported its conclusions, and even viewed in the light most favorable to Cox, the contents of the emails could not be explained away.³⁰⁷⁵ Those emails including the following:

- In 2009, Jason Zabek, Cox's Manager of Customer Abuse Operations, sent an email titled "DMCA Terminations" to the abuse group that said:

"As we move forward in this challenging time we want to hold on to every subscriber we can. With this in mind if a customer is terminated for DMCA, you are able to reactivate them after you give them a stern warning about violating our AUP and the DMCA. We must still terminate in order for us to be in compliance with safe harbor but once termination is complete, we have fulfilled our obligation. After you reactivate them the DMCA 'counter' restarts; The procedure restarts with the sending of warning letters, just like a first offense. This is to be an unwritten semi-policy . . . We do not talk about it or give the subscriber any indication that reactivating them is normal. Use your best judgment and remember to do what is right for our company and subscribers. . . . This only pertains to DMCA violations. It does not pertain to spammers, hackers, etc."

- In a Jan. 2010 email exchange Zabek was asked by an employee what to do with a customer who had progressed through Cox's graduated response procedure and Cox had ultimately determined appropriate circumstances existed to terminate the customer for six months. One month into the termination, the customer was reactivated and soon thereafter, Cox received another notice of infringement tied to the customer. Zabek

³⁰⁷⁴ Id.

³⁰⁷⁵ Id. at 655-56.

responded:

“This is fine. If asked, I would have allowed them back on. We have been turning customers back on who have been terminated for DMCA complaints. As long as our process of warnings, suspen[sion], then termination is followed, we can turn the customer back on and start the DMCA count over. During this time, as we try to keep customers and gain more RGU's [revenue generating units] it is important to try and balance the needs of the company with the protection of the network. DMCA does not hurt the network like DOS attack, spam or hacking. It is not something we advertise however.”

- In August, a representative sent the abuse group an email to confirm that, after a customer is terminated and then reactivated, the next complaint Cox received “is to be treated as a brand new complaint” and the customer is to be “given a clean slate.” Zabek responded:

“Internal info only. Do not forward. After termination of DMCA, if you do suspend someone for another DMCA violation, you are not wrong. However, if the customer has a cox.net email we would like to start the warning cycle over, hold for more, etc. A clean slate if you will. This way, we can collect a few extra weeks of payments for their account. ;-) Once the customer has been terminated for DMCA, we have fulfilled the obligation of the DMCA safe harbor and can start over. . . . We have some leeway here. But know that once a termination happens, we have fulfilled “safe harbor.” These are not in our procedures as we do not make this information publicly known.”

- In March 2011, a customer service representative sent Zabek an email, saying: “Spoke to the customer this morning and he flat out is refusing to do anything on his side and insists nothing is coming from it despite multiple tickets. . . . If possible, please give me some insight on where we should go from this point; ie suspension or something of the sort.” Zabek's instruction was the following:

“You can of course suspend but I would suggest that you just forward any DMCA complaints to his email. . . . He just has to realize that we must send these to him. If a copyright holder dec[ides] to sue, then we want to make sure the customer knows why . . . And it is the law. Make sense? I am not concerned about DMCA and not ready to terminate a CB customer for it . . . yet. It does not cause a big problem on the network. Not like spam, Dos attacks, hacking, etc. do . . . *The customer is doing this on purpose.* I just know it (I can feel it) and is not owned IMO. *They just want to steal stuff . . .*” (emphasis added by the court)

- In an April exchange, a customer service representative sent this inquiry: “This is the customers [sic] third termination. He is waiting call [sic]. What do I tell him when I call him?” Zabek wrote, “DMCA = reactivate,” and then by separate email, “You can make him wait a day or so if you want. ;-)[.]”

- A January 2012 AOL instant messenger conversation between Joseph Sikes, Cox’s Senior Lead Abuse Engineer, and Brent Beck, a software engineer, discussed the meaning of the term, "soft terminate." When asked what a "soft term" was, Sikes explained: "basically, a suspension that is called a termination with the likelihood of reactivation." Then he said, "for DMCA -- we don't want to loose [sic] the revenue." And in response to further questions from Beck, Sikes said, "this is a relatively new process that we've been doing for the past year, again, to retain revenue." Sikes warned Beck that the "Hard/Soft verbiage stays amongst us only. . . . It’s kind of an ‘under the table’ procedure, again, to preserve revenues, when we were loosing [sic] Subscribers, but it only happens about once per month." Finally, a February 2012 email from a Cox employee to the abuse group said, "I was chatting with Daryl and it seems no one has let them know in SAN that *DMCA Terms are not really Terminations any longer.*" (emphasis added by the court)³⁰⁷⁶

The court cited other emails that it found to be of similar ilk. The court noted that under Section 512(i), the penalty imposed by service providers must be termination. Service providers cannot skirt the termination requirement by imposing something short of complete termination of a subscriber or account holder. In view of the cited emails, the court found that Cox did such skirting here, reiterating Zabek’s words that "DMCA = reactivate." Although Cox asserted that its policy had always been to terminate account holders in appropriate circumstances, the court found that such bare assertion was not enough to defeat summary judgment.³⁰⁷⁷ The court cited the Fourth Circuit’s decision in ALS Scan, Inc. v. RemarQ Communities, Inc.,³⁰⁷⁸ stating that the safe harbor immunity is to be granted only to innocent service providers. The district court found that the emails in the record stripped Cox of any innocence and made clear that it was Cox’s policy to intentionally circumvent the DMCA and that its implementation rendered its policy an absolute mirage. The court therefore concluded that no reasonable juror could find that Cox implemented a repeat infringer policy before the fall of 2012.³⁰⁷⁹

The court then turned to an analysis of Cox’s implementation of its repeat infringer policy after the fall of 2012. In October 2012, Cox added two additional suspension steps to its graduated response procedure. BMG conceded that around the same time Cox abandoned its tacit "DMCA = reactivation" policy. Now when Cox terminated a customer, it imposed complete termination of access for six months. For example, in a 2012 email, Sikes wrote, "Now, when we terminate Customers, we REALLY terminate the Customer (for 6 months)." BMG contended, however, that in place of the previous fake terminations, Cox stopped terminating customers altogether, even when Cox knew that a customer was repeatedly and blatantly violating copyrights. As evidence, BMG pointed to a drop-off in the number of terminations following the

³⁰⁷⁶ Id. at 656-58.

³⁰⁷⁷ Id. at 658.

³⁰⁷⁸ 239 F.3d 619, 625 (4th Cir. 2001).

³⁰⁷⁹ Cox, 149 F. Supp. 3d at 658.

policy shift and emails documenting specific instances in which Cox personnel did not terminate account holders despite having knowledge that the account holder was repeatedly infringing.³⁰⁸⁰

The court found that the numbers bore out BMG's first argument. From January 2010 until August 2012, Cox terminated an average of 15.5 account holders a month. Between September 2012 and November 2014 when this suit was filed, Cox terminated an average of 0.8 accounts per month, with a total of 22 terminations. In that same period, Cox took approximately 711,000 customer-facing actions (i.e., it issued 711,000 email warnings and suspensions) in response to alleged infringements. That number did not include the number of first complaints Cox received for each account because Cox took no action on those. Cox also admitted that of the 22 terminated accounts, 17 of them had also either failed to pay their bills on time or were excessive bandwidth users. The court observed that, were these numbers all BMG had, the court could not grant summary judgment. An inference that Cox was not reasonably implementing its policy could be drawn from the numbers, but that conclusion was not compelled by the evidence.³⁰⁸¹

But the court found that BMG also presented evidence of specific instances in which Cox did not terminate account holders despite knowing that they were suing Cox's service to repeatedly infringe, including the following:

- In a March 2014 exchange, a customer service representative wrote, "Customer has been told multiple times that he needs to secure his open wireless router. He has also been warned that the next complaint can result in termination of service." Sikes responded, "Yep, this is their absolute last chance to either secure their wireless router and/or remove ALL P2P clients from their systems. Next complaint = 6 month termination." A few weeks later, the same service representative emailed to say, "Last ticket . . . customer was warned that further complaints would result in termination. We have received an additional complaint."

Sikes responded: "[I]t looks like the Customer suspected that their wireless network was the culprit. I assume you also covered the likely possibility that it could also be a BitTorrent client running on one of their computers? If this was not covered thoroughly in the last call with them, please advise them that securing their wireless network obviously did not work. So, the BitTorrent client is running on one of their computers (their child's, etc.) and they need to uninstall it. This customer pays us over \$400/month and if we terminate their service, they will likely cancel the rest of their services. Every terminated Customer becomes lost revenue and a potential Detractor to our Net Promoter Score. We should make absolutely certain that we have covered each and every possibility with them ("to the bitter end") before we terminate them. If all of this has been covered in detail, then please go ahead and terminate their internet service for this complaint.

³⁰⁸⁰ Id. at 658-59 & n.16.

³⁰⁸¹ Id. at 659.

The rep responded, "Looks like PTP programs were discussed back on ticket 15711339 (Which was also a final suspension as well)." Sikes responded, "That was back in October 2013 [approximately five months earlier]. We can't expect our Customers to know and remember as much as we do about this stuff, especially if the account holder is not the one using BitTorrent. . . . On this Customer's last suspension . . . , at the beginning of this month (March 5th), did you also explain that they should still check all of the computers in their household for BitTorrent clients and to speak with other members of their household . . . about running/installing BitTorrent and downloading/sharing files? You only mentioned their wireless network in your work log notes. On final suspensions, we need to be as detailed as possible on the work log notes, show that we have covered EVERYTHING with the Customer. On 404 suspensions for DMCA,³⁰⁸² this is our last ditch effort to save the Customer. Obviously, if they don't care and don't want to help us help them, there's not much more we can do, but this should also be noted in the work log notes."

After a service representative responded that the customer had been told about file sharing and torrents, Sikes decided, "Please suspend this Customer, one LAST time.

- In May, a representative sent an email to the abuse group that said, "Request for termination review – Cats Ticket 19991279. This is the 3rd time to the 404 number. Was warned on last call that next offense would result in termination review. Notes indicate that customer was advised to remove file sharing program on last call." Sikes responded, "Since this Customer knows 'it's his fault', please ask this Customer what he will do to prevent this from happening again and note it in the ticket work log. Then let him know that one more complaint will result in a 6 month Termination."
- In June, a senior engineer in the abuse group said this about a customer who had been given a final suspension and advised to remove all P2P file-sharing programs: "This customer will likely fail again, but let's give him one more change [sic]. [H]e pays 317.63 a month." Also in June, a customer service representative emailed the abuse group about a different customer, saying, "This customer is well aware of his actions and is upset that 'after years of doing this' he is now getting caught. Customer was advised to stop sharing, check his wireless and remove his PTP programs." Sikes responded, "Please advise this Customer that this is their final termination & reactivation. If we receive one more complaint, we will, regretfully, not be able to provide them with data service for 6 months."³⁰⁸³

³⁰⁸² "404" referred to the area code in Atlanta, Georgia, which meant the customer had been through the final suspension steps where he or she was required to speak with Cox's high-level customer service representatives. Id. at 660 n.18.

³⁰⁸³ Id. at 659-60.

Based on these exchanges in the record, the court found that BMG had identified specific instances in which Cox knew accounts were being used repeatedly for infringing activity yet failed to terminate, and that Cox had not seriously challenged those examples. Cox argued that the cited snippets of conversations did not show what actions call centers actually took against accounts. The court noted, however, that in its view Cox had been careful never to assert that those customers were in fact terminated. And BMG noted that not one of those subscribers or their abuse ticket numbers could be found on the list of terminated subscribers that Cox had produced in discovery.³⁰⁸⁴

The court noted that Cox appeared to be hanging its hat on the notion that an “infringer” for purposes of the DMCA safe harbors is someone who has been adjudicated an infringer in court. Working from that premise, the court understood Cox to be arguing that as a matter of choice and not obligation, Cox had chosen to apply its graduated response procedures to mere accusations involving its accounts, so that Cox’s policy went above and beyond what the DMCA required and its failure to act based on notices of infringement could not render Cox ineligible for the safe harbor’s protection. Cox also argued that by not defining “appropriate circumstances,” Congress had left it to the service provider to make its own determination of when such circumstances exist.³⁰⁸⁵

The court rejected Cox’s arguments, observing that although Cox was under no duty to monitor for infringement, it did not have leeway to wait until an account holder was adjudicated as an infringer to find that circumstances were appropriate for termination. Rather, an account holder must be considered an infringer, at minimum, when the service provider has actual knowledge that the account holder is using its services for infringing purposes. Appropriate circumstances arise when an account holder is repeatedly or flagrantly infringing copyrights. Thus, when Cox had actual knowledge of particular account holders who blatantly or repeatedly infringed, the responsibility shifted to Cox to terminate their accounts.³⁰⁸⁶

The court noted an additional argument by Cox that knowledge of infringement cannot be established by notices submitted by copyright holders because they can be unreliable for a variety of reasons. The court noted conflicting authority as to whether notices of infringement should be considered evidence sufficient to give a service provider knowledge of a user’s infringement.³⁰⁸⁷ But whether or not DMCA-compliant notices are sufficient, standing alone, to establish a service provider’s knowledge for purposes of the safe harbor, the court noted that they are powerful evidence of a service provider’s knowledge, citing the Ninth Circuit’s decision in Shelter Capital Partners LLC.³⁰⁸⁸ Moreover, the court noted that the account holders referenced in the cited emails had already been through Cox’s entire graduated response

³⁰⁸⁴ Id. at 661.

³⁰⁸⁵ Id.

³⁰⁸⁶ Id.

³⁰⁸⁷ Id.

³⁰⁸⁸ Id. at 662 (citing UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1020 (9th Cir. 2013)).

procedure, meaning that Cox had received at least fourteen infringement notices tied to their accounts in a six-month period. And Cox customer service representatives worked with those customers on each of their four hard-walled garden suspensions to identify the cause of the infringement notices, including the possibilities of malware, an unsecured wireless network, or a file-sharing program on another computer in the household. The court therefore concluded that by the time an account holder reached the end of Cox's graduated response procedure, the chance that the account holder was not a willful infringer was substantially lessened.³⁰⁸⁹

Finally, and critically, the court noted that the emails in the record revealed that Cox had knowledge that at least some of its account holders were intentionally and repeatedly infringing. It was therefore clear that Cox was able to tell from its account holders' statements and conduct referenced in those emails that infringement was occurring. Yet, Cox continued to provide service to them. Accordingly, the court concluded that Cox had not come forward with any evidence that would raise a genuine issue of material fact as to whether it had unreasonably implemented its repeat-infringer policy by failing to terminate users who repeatedly or blatantly infringed copyright. The court therefore ruled that BMG was entitled to summary judgment on Cox's safe harbor defense, and that if Cox were determined to be liable for contributory or vicarious copyright infringement, BMG would not be limited in the remedies it could seek.³⁰⁹⁰

After the close of discovery, Cox moved for summary judgment on five grounds: (1) whether there was evidence of direct infringement by third parties with respect to which Cox could be secondarily liable; (2) whether there was evidence of Cox's contributory infringement; (3) whether there was evidence of Cox's vicarious liability; (4) whether BMG failed to mitigate its damages; and (5) whether BMG's unclean hands barred its claims. For the reasons discussed in Section III.C.2(w) above, the court found summary judgment inappropriate on the first four grounds, but ruled that Cox's defense of unclean hands failed as a matter of law. The court then allowed the case to proceed to trial before a jury. On Dec. 17, 2015, the jury returned a verdict finding Cox liable for contributory infringement and finding that Cox's infringements were willful, but finding Cox not liable for vicarious infringement. The jury awarded BMG \$25,000,000 in statutory damages, or approximately \$18,000 per infringed work.³⁰⁹¹

After the verdict, Cox moved for judgment as a matter of law or, in the alternative, a new trial, and BMG moved for judgment as a matter of law on its claim of vicarious infringement as well as for permanent injunctive relief.³⁰⁹² The court denied all post-trial motions for the reasons set forth in Section III.C.2(w) above.

³⁰⁸⁹ Cox, 149 F. Supp. 3d at 662.

³⁰⁹⁰ Id.

³⁰⁹¹ See Eriq Gardner, "Music Publisher Gets \$25 Million Jury Verdict Against Cox in Trailblazing Piracy Case," available as of Dec. 17, 2015 at www.billboard.com/articles/business/6813610/bmg-25-million-jury-verdict-cox-piracy. The jury's verdict form may be found at www.documentcloud.org/documents/2648509-BMG-Verdict.html.

³⁰⁹² BMG Rights Mgmt. (US) LLC v. Cox Comm'ns, Inc., 2016 U.S. Dist. LEXIS 105981 (E.D. Va. Aug. 8, 2016).

The Fourth Circuit's Decision

On appeal, the Fourth Circuit affirmed the district court's grant of summary judgment that Cox was not entitled to the DMCA safe harbor.³⁰⁹³ (The Fourth Circuit's rulings with respect to contributory liability and other issues related to common law liability are discussed in Section III.C.2(w) above.) Cox's principal contention on appeal was that "repeat infringers" in Section 512(i)(1)(A) means adjudicated repeat infringers – i.e., persons who have been held liable by a court for multiple instances of copyright infringement. The Fourth Circuit rejected this argument for several reasons. First, because the DMCA does not define the term, the court looked to its ordinary meaning, which it defined simply as one who infringes a copyright more than once. Cox contended that because the repeat infringer provision uses the term "infringer" without modifiers such as "alleged" or "claimed" that appear elsewhere in the DMCA, "infringer" must mean "adjudicated infringer." The court ruled, however, that the DMCA's use of phrases like "alleged infringer" in other portions of the statute indicated only that the term "infringer" alone must mean something different from "alleged infringer," otherwise the word "alleged" would be superfluous. Using the ordinary meaning of "infringer," however fully accorded with this principle: someone who actually infringes a copyright differs from someone who has merely allegedly infringed a copyright, because an allegation could be false. The court therefore concluded that the need to differentiate the terms "infringer" and "alleged infringer" did not mandate Cox's proposed definition.³⁰⁹⁴

The court further noted that other provisions of the Copyright Act use the term "infringer" and similar terms to refer to all who engage in infringing activity, not just the narrow subset of those who have been so adjudicated by a court. Similarly, Section 512(g)(1) provides that OSPs who store copyrighted material are generally not liable for removing material or activity "claimed to be infringing" or based on facts or circumstances from which "infringing activity is apparent," regardless of whether the material or activity is "ultimately determined to be infringing." The distinction between "infringing activity" and activity "ultimately determined to be infringing" in Section 512(g)(1) thus shelters OSPs from being liable for taking down material that is "infringing," even if no court "ultimately determine[s]" that it is infringing – because, for example, the copyright holder simply does not file a lawsuit against the person who uploaded the infringing material. The court noted that Section 512(g)(1) therefore illustrates that Congress knew how to expressly refer to adjudicated infringement, but did not do so in the repeat infringer provision of Section 512(i).³⁰⁹⁵ The court found the legislative history to reinforce its conclusion in a passage in the House Report stating that if persons abuse their access to the Internet through disrespect for the intellectual property rights of others, they should face a realistic threat of losing their Internet access. The passage did not suggest that they should risk losing Internet access only once they had been sued in court and found liable for

³⁰⁹³ BMG Rights Mgmt. (US) LLC v. Cox Comm'ns, Inc., 881 F.3d 293 (4th Cir. 2018).

³⁰⁹⁴ Id. at 301.

³⁰⁹⁵ Id. at 301-02.

multiple instances of infringement. The court therefore rejected Cox's argument that the term "repeat infringers" in Section 512(i) is limited to adjudicated infringers.³⁰⁹⁶

The court then turned to whether Cox had reasonably implemented a policy that provides for the termination in appropriate circumstances of its subscribers who repeatedly infringe copyrights. Although OSPs have flexibility in determining when it is appropriate to terminate a person's access to the Internet, the court noted that, at a minimum, an OSP has not reasonably implemented a repeat infringer policy if the OSP fails to enforce the terms of its policy in any meaningful fashion. Such was the case here. Cox formally adopted a repeat infringer policy, but, both before and after September 2012, the evidence established that it made every effort to avoid reasonably implementing that policy. In carrying out its thirteen-strike process, Cox very clearly determined not to terminate subscribers who in fact repeatedly violated the policy.³⁰⁹⁷

Citing many of the same emails among Cox employees cited by the district court (as discussed above), the court found that Cox's actual practice from the beginning of the litigated time period until September 2012 was never to terminate a subscriber for infringement without shortly thereafter reactivating them. The court rejected Cox's argument that it lacked actual knowledge of its subscribers' infringement and therefore did not have to terminate them, noting that the evidence showed Cox always reactivated subscribers after termination, regardless of its knowledge of the subscriber's infringement. The court ruled that an OSP cannot claim the DMCA safe harbor merely by terminating customers as a symbolic gesture before indiscriminately reactivating them within a short timeframe.³⁰⁹⁸

The court noted the evidence further showed that, in September 2012, Cox abandoned its practice of routine reactivation and adopted a policy to terminate for real. But instead of terminating and then reactivating subscribers, Cox simply stopped terminating them in the first place. The court noted that before September 2012, Cox was terminating (and reactivating) 15.5 subscribers per month on average; after September 2012, Cox abruptly began terminating less than one subscriber per month on average. Moreover, Cox dispensed with terminating subscribers who repeatedly infringed BMG's copyrights in particular when it decided to delete automatically all infringement notices received from BMG's agent, Rightscorp, which amounted to millions of notices. The court noted that, although the relevant inquiry concerned Cox's policy toward all of its repeatedly infringing subscribers, not just those who infringed BMG's copyrights, Cox's decision to categorically disregard all notices from Rightscorp provided further evidence that Cox did not reasonably implement a repeat infringer policy.³⁰⁹⁹

³⁰⁹⁶ Id. at 302 (citing H.R. Rep. No. 105-551, pt. 2, at 61 (1998)).

³⁰⁹⁷ Id. at 303.

³⁰⁹⁸ Id. at 303-04.

³⁰⁹⁹ Id. at 304.

BMG also provided evidence of particular instances in which Cox failed to terminate subscribers whom Cox itself regarded as repeated infringers, as demonstrated by internal emails of Cox employees. Cox argued that these post-September 2012 emails did not necessarily *prove* actual knowledge of repeat infringement. The court rejected this argument, noting that Cox bore the burden of proof on the DMCA safe harbor defense, and it therefore had to point to evidence showing that it reasonably implemented a repeat infringer policy. The emails showed that Cox internally concluded that a subscriber should be terminated after the next strike, but then declined to do so because it did not want to lose revenue. The court rejected Cox's argument that the emails concerned only four cases, and that occasional lapses are forgivable. The court noted that even four cases were significant when measured against Cox's equally small total number of relevant terminations during the period of the emails – also four. More importantly, Cox did not produce any evidence of instances in which it *did* follow through on its policy and terminate subscribers after giving them a final warning to stop infringing. Nor had Cox provided any evidence that a determination of “appropriate circumstances” played *any* role in its decisions to terminate or not to terminate. Cox did not, for example, point to any criteria that its employees used to determine whether appropriate circumstances for termination existed. Instead, the evidence showed that Cox's decisions not to terminate had nothing to do with appropriate circumstances, but instead were based on one goal – not losing revenue from paying subscribers. Accordingly, the Fourth Circuit ruled that the district court correctly granted summary judgment to BMG that Cox was not entitled to the safe harbor defense.³¹⁰⁰

(ii) Caching – Section 512(b)

Section 512(b) provides that a Service Provider is not liable for monetary relief, and is subject only to limited injunctive relief, for caching (i.e., what Section 512(b) calls the “intermediate and temporary storage”) of material on a system or network operated by the Service Provider which was made available online by a person other than the Service Provider.³¹⁰¹ Such caching must occur through an automatic technical process upon the original

³¹⁰⁰ *Id.* at 304-05.

³¹⁰¹ Section 512(b) provides: “(1) Limitation on liability – A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which –

(A) the material is made available online by a person other than the service provider;

(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of the other person; and

(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A),

if the conditions set forth in paragraph (2) are met.

(2) Conditions – The conditions referred to in paragraph (1) are that –

transmission of such material to a requester, in order to make the material available to subsequent persons requesting it from the person who first made it available online. Thus, the literal language of Section 512(b) appears not to cover “advance” caching, in which material is copied into a cache for anticipated requests for it, rather than upon the first actual request for it,³¹⁰² although the cases of Field v. Google and Parker v. Google, discussed in the next subsections, reached a contrary result.

(A) the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A);

(B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies;

(C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology –

(i) does not significantly interfere with the performance of the provider’s system or network or with the intermediate storage of the material;

(ii) is consistent with generally accepted industry standard communications protocols; and

(iii) does not extract information from the provider’s system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person;

(D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions; and

(E) if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if –

(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and

(ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled.”

³¹⁰² See also H.R. Rep. No. 105-551 Part 2, at 52 (1998): “For subsection (b) to apply, the material must be made available on an originating site, transmitted at the direction of another person through the system or network operated by or for the service provider to a different person, and stored through an automatic technical process so that users of the system or network who subsequently request access to the material from the originating site may obtain access to the material from the system or network.”

In addition, the safe harbor requires that the Service Provider must (i) not modify the cached material; (ii) comply with all rules of the originator of the material for refreshing, reloading or other updating of the cached material in accordance with a generally accepted industry standard data communications protocol (provided such rules are not used by the originator to unreasonably impair intermediate storage); (iii) not interfere with any technology associated with the cached material that returns information to the originator (such as cookies) that would have been obtained in the absence of transmission through caching (provided such technology does not interfere with the performance of the system or network, is consistent with accepted industry standard communications protocols, and does not extract other information from the system or network); (iv) if the originator has conditioned access to the information, such as upon payment of a fee or provisions of a password, permit access to the cached information “in significant part”³¹⁰³ only upon the same conditions; and (v) respond expeditiously to remove or disable access to any cached information upon receipt of notice that such information has been removed or disabled from the originating site (or ordered by a court to be removed) from which the information was cached.

a. **Field v. Google**

The facts of the case of Field v. Google³¹⁰⁴ are set forth in Section III.B.4(a) above. In that case, the court ruled that Google was entitled to the Section 512(b) safe harbor for its activities of caching web sites through its Web crawler known as the “Googlebot” and making the cached copies of particular pages available for download directly from Google’s computers by end users clicking on the “Cached” link to a web page contained in search results returned by Google’s search engine.

The court rejected a number of arguments by the plaintiff, Field, concerning why Google should not be entitled to the Section 512(b) safe harbor. First, Field contended that, in operating its cache, Google did not make “intermediate and temporary storage” of the cached material, as required by Section 512(b)(1). The court cited the Ellison v. Robertson case,³¹⁰⁵ involving the Section 512(a) safe harbor, which ruled that AOL’s storage of Usenet postings for about 14 days was both “intermediate” and “transient” as required by Section 512(a). Analogizing to that case, the court noted that the copy of Web pages Google stored in its cache were present for approximately 14 to 20 days. The court found that this period was sufficiently short to be deemed “temporary” under Section 512(b).³¹⁰⁶

In a significant aspect of its ruling, the court also implicitly held that, to qualify for the Section 512(b) safe harbor, the caching need not be done only after a user has made an initial request for the materials being cached, but could be done in anticipation of user requests for the

³¹⁰³ This language appears to have been inserted in recognition of the fact that hackers or others may be able to circumvent such restrictions on access without knowledge of the Service Provider. Id. at 7.

³¹⁰⁴ 412 F. Supp. 2d 1106 (D. Nev. 2006).

³¹⁰⁵ 357 F.3d 1072, 1081 (9th Cir. 2004).

³¹⁰⁶ Field v. Google, 412 F. Supp. 2d at 1124.

materials: “Like AOL’s repository of Usenet postings in Ellison which operated between the individuals posting information and the users requesting it, Google’s cache is a repository of material that operates between the individual posting the information, and the end-user requesting it.”³¹⁰⁷

Field also contended that Google’s cache did not satisfy the requirements of Section 512(b)(1)(B) that the material in question be transmitted from the person who makes it available online, here the plaintiff, to a person other than himself, at the direction of the other person.³¹⁰⁸ The court rejected this argument: “Field transmitted the material in question, the pages of his Web site, to Google’s Googlebot at Google’s request. Google is a person other than Field. Thus, Google’s cache meets the requirement of Section 512(b)(1)(B).”³¹⁰⁹ Here the court appears to have misidentified the parties that Section 512(b)(1)(B) is directed to, although the misidentification would not seem to change the conclusion that Section 512(b)(1)(B) is satisfied. Specifically, the court’s quoted language treats Google as the “other person.” However, because Google is acting as the service provider, it should not be treated as the “other person.” Rather, Google’s users are the “other persons” to whom Section 512(b)(1)(B) appears to be directed.

Finally, Field contended that Google’s cache did not fully satisfy the requirements of Section 512(b)(1)(C) requiring that Google’s storage of Web pages be carried out through “an automated technical process” and be “for the purpose of making the material available to users ... who ... request access to the material from [the originating site].”³¹¹⁰ The court rejected this argument, noting that Field’s complaint stated that third party web page content was added to the Google cache by an automated software process. Nor was there any dispute that one of Google’s principal purposes in including Web pages in its cache was to enable subsequent users to access those pages if they were unsuccessful in requesting the materials from the originating site for whatever reason, which was sufficient to meet the requirements of Section 512(b)(1)(C). Accordingly, the court granted Google’s motion for partial summary judgment that it qualified for the Section 512(b) safe harbor.³¹¹¹

b. Parker v. Google

In Parker v. Google,³¹¹² the court ruled, citing Field v. Google, that Google had immunity under Section 512(b) for claims of direct infringement based on Google’s automatic caching of USENET messages, including an excerpt of the plaintiff’s copyrighted work that he had posted to USENET, as a means of indexing web sites and producing results to search queries.³¹¹³ Similar to

³¹⁰⁷ Id.

³¹⁰⁸ Id.

³¹⁰⁹ Id.

³¹¹⁰ Id.

³¹¹¹ Id. at 1124-25.

³¹¹² 422 F. Supp. 2d 492 (E.D. Pa. 2006), aff’d, 2007 U.S. App. LEXIS 16370 (3d Cir. July 10, 2007).

³¹¹³ Id. at 497-98. The issue of immunity under Section 512(b) was not addressed by the Third Circuit on appeal.

Field v. Google, the court did not impose any requirement that, to qualify for the Section 512(b) safe harbor, the caching must be done only after a user has made an initial request for the materials being cached, but rather could be done in anticipation of user requests for the materials.

c. Perfect 10 v. Google

In Perfect 10 v. Google,³¹¹⁴ Perfect 10 alleged that Google infringed on its copyrights in pictures of nude models by caching portions of websites that hosted infringing images, by linking to third party websites that hosted infringing images, and by hosting infringing images on its own servers that had been uploaded by users of Google's "Blogger" service. On remand from the Ninth Circuit with respect to issues of common law secondary liability and fair use (see discussion in Section II.C.4 above), Google moved for summary judgment that it was entitled to the safe harbors under Sections 512(b), (c) and (d).³¹¹⁵

The court first turned to the preliminary issues of whether Google satisfied the safe harbor threshold condition of implementation of a suitable repeat infringer policy and whether Perfect 10's notices were adequate. With respect to a suitable repeat infringer policy, Google had a system for receiving and processing notifications of infringement and would terminate an account holder on its Blogger service if it determined that three DMCA notices of infringement against that blogger were valid.³¹¹⁶ With respect to its Web Search and Image Search services, Google did not have account holders, but that fact did not eliminate eligibility for the safe harbors: "Google points out – and P10 does not dispute – that Web Search, Image Search, and the caching feature do not have account holders or subscribers. P10 does not contend that Google must, or even can, have a repeat infringer policy for those services. *See 17 U.S.C. § 512(i)(1)(A)* (requiring a repeat infringer policy for those services with 'subscribers and account holders')." ³¹¹⁷ The court rejected a challenge by Perfect 10 to the adequacy of Google's repeat infringer policy with respect to the Blogger service based on the fact that Google tracked only email addresses, not the actual names of users. The court held that the DMCA does not impose an obligation on service providers to track their users in any particular way.³¹¹⁸

Turning to Google's assertion of the Section 512(b) safe harbor, the court noted that it was undisputed that Google's cache servers did not store images found on a cached page, only the text – images displayed on a cached page were made available to a viewer by links to their original source, if they still existed at that source. Accordingly, Perfect 10's claims for infringement based on images "located in" Google's cache were really claims based on Google's

³¹¹⁴ 2010 U.S. Dist. LEXIS 75071 (C.D. Cal. July 26, 2010), aff'd, 653 F.3d 976, 978 (9th Cir. 2011), cert. denied, 132 S. Ct. 1713 (2012).

³¹¹⁵ Id. at *2-3.

³¹¹⁶ Id. at *7, 13.

³¹¹⁷ Id. at *13.

³¹¹⁸ Id. at *14.

linking to outside infringing content, to which the Section 512(d) safe harbor would be relevant.³¹¹⁹ In any event, the court noted that in none of Perfect 10's relevant notices of infringement did it identify any specific material in Google's cache as infringing, so its notices were deficient as to the cached pages. The court also rejected Perfect 10's argument that a notice identifying a web page necessarily identifies the cached page as well. Accordingly, the court ruled that it need not decide whether Google would be separately entitled to the Section 512(b) safe harbor for its caching activity, in addition to the Section 512(d) safe harbor for linking to allegedly infringing images through its cached pages.³¹²⁰

Turning to the applicability of the Section 512(d) safe harbor to Google's Web Search and Image Search services, the court examined in detail the adequacy under DMCA requirements of Perfect 10's notices of infringement.³¹²¹ The litigants divided those notices into Groups A, B, and C, based on when they were sent to Google. The Group A notices were all sent by email to webmaster@google.com instead of to the address of Google's designated agent listed at the Copyright Office and were otherwise deficient for not identifying specifically which copyrighted works were infringed. Accordingly, the Group A notices were inadequate to disqualify Google from the Section 512(d) safe harbor.³¹²²

With respect to the Group B notices, the court held that Google had not met its burden of showing that there was no dispute of material fact as to whether these notices were valid under the DMCA. Each notice contained references to dozens or even hundreds of alleged infringing links. Google argued that the notices were invalid in their entirety because the majority of the references were invalid since they contained incomplete URLs, lacked image-specific URLs, or did not reference the copyrighted work with specificity. The court agreed that references having those deficiencies did not confer adequate notice under the DMCA and Google was not required to act to remove any entry that did not meet the DMCA requirements. However, other Group B notices did meet all of the requirements of the DMCA, such as one that contained a complete URL along with the volume, issue, and page number of the *Perfect 10* magazine in which the image originally appeared. The court noted that the Group B notices enabled Google to scan the entries to determine their compliance with the DMCA and it would not be an undue burden on Google to do so. In addition, Perfect 10 offered evidence that in some instances Google waited between four and seventeen months to process a number of the Group B notices, as well as evidence that some notices were not processed at all.³¹²³ Accordingly, the court denied Google's motion for summary judgment "as to safe harbor for at

³¹¹⁹ *Id.* at *5-6, *37.

³¹²⁰ *Id.* at *38 & n.10, *45.

³¹²¹ Perfect 10 did not argue that Google received a direct financial benefit from the infringing activity, had the right and ability to control such activity, and thus could not enjoy safe harbor protection for its web and image search results. *Id.* at *20.

³¹²² *Id.* at *22.

³¹²³ *Id.* at *22-26.

least some of the Group B notices.”³¹²⁴ Significantly, this statement suggests that the DMCA safe harbors are to be applied on a notice-by-notice basis.

The Group C notices, like those notices at issue in the Ninth Circuit’s CCBill case, required Google to move back and forth between several different files in order to determine whether a given URL was infringing. The Group C notices generally consisted of a cover letter, a spreadsheet, and a hard drive or DVDs containing electronic files. Where Perfect 10 provided spreadsheets, the spreadsheets did not identify the infringing URL, but merely the top-level URL for the entire website. The court noted that Perfect 10 apparently expected Google to comb through hundreds of nested electronic folders containing over 70,000 distinct files, including raw image files such as JPEG files and screen shots of Google search results, in order to find which link was allegedly infringing. In many cases, the file containing the allegedly infringing image did not even include a URL, or the URL was truncated. The spreadsheets also did not identify the copyrighted work that was allegedly infringed – Google would have been required to search through a separate electronic folder supplied by Perfect 10 with its cover letter to the notice of infringement containing all of the more than 15,000 images that appeared on Perfect 10’s website as of June 2007, in order to identify the copyrighted work that was infringed. Thus, no single document of any of the Group C notices contained all of the information required in a valid DMCA notification, and the court ruled that the Group C notices were therefore deficient. Accordingly, the court concluded that Perfect 10 had not raised a genuine issue of material fact as to whether Google was eligible for safe harbor under Section 512(d) with respect to the Group C notices.³¹²⁵

Next, the court turned to whether Google was entitled to the Section 512(c) safe harbor with respect to its Blogger service, which some of its account holders had used to upload allegedly infringing images onto Google’s servers. With respect to the Group B notices, the court noted that Perfect 10 had not contended in either its opposition papers or in oral argument that Google had failed to expeditiously process even a single Blogger URL identified within the Group B notices. With respect to the Group C notices, the court noted that the requirements for a copyright holder are slightly less stringent under Section 512(c) than under Section 512(d) in that the former does not explicitly require the copyright holder to provide what the latter does, a specific “identification of the reference or link” to material or activity claimed to be infringing. Section 512(c) merely requires the copyright holder to provide “identification of the material that is claimed to be infringing ... and information reasonably sufficient to permit the service provider to locate the material.” Nevertheless, the court noted that Google had a tenable argument that a copyright holder would need to provide the post-URL of a particular Blogger post in order to constitute information “reasonably sufficient” to permit the location of the material. However, the court decided it need not address that argument, since the other manifest deficiencies in the Group C notices – including the lack of specific identification of the

³¹²⁴ Id. at *27.

³¹²⁵ Id. at *27-36.

copyrighted material and their unduly complicated organization – prevented them from imparting knowledge under the statute.³¹²⁶

Finally, the court addressed whether Google was ineligible for the Section 512(c) safe harbor because it received a financial benefit directly attributable to infringing activity that Google had the right and ability to control. Perfect 10's only argument that Google had a right and ability to control the infringing activity on Blogger was that the infringing material was on Google's servers and Google could take it down. The court ruled that the mere ability of a service provider to remove content after it had been uploaded was insufficient as a matter of law to establish the right and ability to control infringing activity. Accordingly, Google had demonstrated that it was entitled to the Section 512(c) safe harbor for its Blogger service as a matter of law.³¹²⁷

In sum, the Court granted in part and denied in part Google's motion for partial summary judgment of entitlement to safe harbor under Section 512(d) for its Web and Image Search, granted Google's motion for partial summary judgment for its caching feature based on Section 512(d), without having to assess whether it would be separately entitled to safe harbor under Section 512(b), and granted Google's motion for partial summary judgment of entitlement to safe harbor under Section 512(c) for its Blogger feature.³¹²⁸

The district court also denied Perfect 10's motion for a preliminary injunction on the basis that it had not shown it was likely to suffer irreparable harm in the absence of such relief, and that it had failed to satisfy any of the other requirements for a preliminary injunction.³¹²⁹ On appeal, Perfect 10 claimed the district court erred in denying its motion for a preliminary injunction and sought review of the district court's summary judgment order under the safe harbors, arguing that the order was inextricably intertwined with its request for a preliminary injunction.³¹³⁰

The Ninth Circuit affirmed the district court's denial of a preliminary injunction. First, the court ruled that, following the Supreme Court's decision in eBay Inc. v. MercExchange, LLC,³¹³¹ "the propriety of injunctive relief in cases arising under the Copyright Act must be evaluated on a case-by-case basis in accord with traditional equitable principles and without the aid of presumptions or a 'thumb on the scale' in favor of issuing such relief."³¹³² Although eBay dealt with a permanent injunction, the Ninth Circuit concluded that the rule enunciated in that case is

³¹²⁶ Id. at *40-43.

³¹²⁷ Id. at *43-44.

³¹²⁸ Id. at *45.

³¹²⁹ Perfect 10, Inc. v. Google, Inc., 653 F.3d 976, 978 (9th Cir. 2011), cert. denied, 132 S. Ct. 1713 (2012).

³¹³⁰ Id.

³¹³¹ 547 U.S. 388 (2006).

³¹³² Perfect 10 v. Google, 653 F.3d at 980. The Ninth Circuit was persuaded by the Second Circuit's reasoning when it reached the same conclusion in the case of Salinger v. Colting, 607 F.3d 68, 75, 79 (2d Cir. 2010).

equally applicable to preliminary injunctive relief.³¹³³ The court then affirmed the district court's denial of a preliminary injunction because Perfect 10 had not shown a sufficient causal connection between its business harm and Google's operation of its search engine. Perfect 10 argued that its revenues had declined from nearly \$2 million per year to less than \$150,000 per year during the period in which thumbnails of Perfect 10's images had become more widely available through Google's search engine, and that Perfect 10 was very close to bankruptcy. The Ninth Circuit held this was insufficient evidence to establish that failure to enjoin Google's operations would cause Perfect 10 irreparable harm. First, Perfect 10 had not alleged that it was ever in sound financial shape, and the company's president and founder acknowledged that search engines other than Google contributed to making Perfect 10 images freely available. In addition, Perfect 10 had failed to submit a statement from even a single former subscriber who ceased paying for Perfect 10's service because of the content freely available via Google. Accordingly, the Ninth Circuit affirmed the denial of a preliminary injunction.³¹³⁴

(iii) Innocent Storage of Infringing Information – Section 512(c)

Section 512(c) provides that a service provider is not liable for monetary relief, and is subject only to limited injunctive relief, for storage at the direction of a user of infringing material on its system or network where the service provider does not have actual knowledge that the material is infringing; is not aware of facts or circumstances from which infringing activity is apparent; does not receive a financial benefit directly attributable to any infringing activity for which it has the right and ability to control; and, if properly noticed of the infringing activity by the copyright holder or its authorized agent, or otherwise obtaining knowledge or awareness of the infringement, responds expeditiously to remove or disable access to the infringing material.³¹³⁵

³¹³³ Perfect 10 v. Google, 653 F.3d at 981.

³¹³⁴ Id. at 981-82.

³¹³⁵ Section 512(c) provides: "A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider –

(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity."

The service provider can become aware of infringing activity either by notice from the copyright holder (or its authorized agent) or by virtue of other facts or circumstances of which it becomes aware. Absent direct notice from the copyright holder or its agent, the standard of awareness of infringing activity appears by its terms to require more knowledge on the part of the service provider than a “should have known” (or reason to know) standard. Specifically, it requires that the service provider have actual awareness of facts from which infringing activity is apparent. The legislative history describes the standard of awareness as a “red flag” test. “[I]f the service provider becomes aware of a ‘red flag’ from which infringing activity is apparent, it will lose the limitation of liability if it takes no action. The ‘red flag’ test has both a subjective and an objective element. In determining whether the service provider was aware of a ‘red flag,’ the subjective awareness of the service provider of the facts or circumstances in question must be determined. However, in deciding whether those facts or circumstances constitute a ‘red flag’ – in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances – an objective standard should be used.”³¹³⁶

Section 512(c)(3) specifies the requirements for proper notice of infringement by the copyright holder to the Service Provider, which constitutes a written communication provided to the designated agent of the Service Provider that includes “substantially” the following:³¹³⁷

³¹³⁶ H.R. Rep. No. 105-551 Part 2, at 53 (1998).

³¹³⁷ Section 512(c)(3) provides: “Elements of notification –

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(B)(i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.

- identification of the copyrighted work or a representative list of works at the site (if multiple copyrighted works at a single online site are covered by a single notification);³¹³⁸
- identification of the infringing material in sufficient detail to permit the Service Provider to locate the material;
- information (including an e-mail address) where the complaining party can be contacted; and
- a statement signed by physical signature or electronic signature under penalty of perjury that the complaining party has the authority to enforce the rights that are claimed to be infringed and a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

Section 512(c)(3)(B)(ii) provides that, if a notice complies with at least the first three of the preceding requirements, then in order to take advantage of the safe harbor, the Service Provider must promptly attempt to contact the complaining party or take other reasonable steps to assist in the receipt of notification that substantially complies with all the preceding requirements for notice.

The DMCA does not define what constitutes a “direct financial benefit” from the infringing activity, but presumably the mere receipt of monthly subscription fees from the infringing user would not be a “direct” financial benefit from the infringing activity.³¹³⁹ It is also unclear what constitutes sufficient “right and ability to control” the infringing activity. Most Service Providers impose certain rules on the users of their system, but, as a practical matter, do not and are not able to control the myriad individual actions of users of the system. The same

(ii) In a case in which the notification that is provided to the service provider’s designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).”

³¹³⁸ A notice may cover multiple works: “Where multiple works at a single on-line site are covered by a single notification, a representative list of such works at that site is sufficient.” H.R. Rep. No. 105-551 Part 2, at 55 (1998); see 17 U.S.C. § 512(c)(3)(A)(ii). What constitutes an adequate “representative list” of works was adjudicated in the case of ALS Scan, Inc. v. RemarQ Communities, Inc., 239 F.3d 619 (4th Cir. 2001), discussed below.

³¹³⁹ “In general, a service provider conducting a legitimate business would not be considered to receive a ‘financial benefit directly attributable to the infringing activity’ where the infringer makes the same kind of payment as noninfringing users of the provider’s service. Thus, receiving a one-time set-up fee and flat, periodic payments for service from a person engaging in infringing activities would not constitute receiving a ‘financial benefit directly attributable to the infringing activity.’ Nor is subsection (c)(1)(B) intended to cover fees based on the length of the message (e.g., per number of bytes) or by connect time. It would however, include any such fees where the value of the service lies in providing access to infringing material.” H.R. Rep. No. 105-551 Part 2, at 54 (1998).

phrase – “right and ability to control” – appears in the safe harbor of Section 512(d) as well, which was asserted in the Napster case, as discussed in subsection (iv) below.

Finally, to take advantage of this safe harbor, the OSP must designate an agent to receive notifications of claimed infringements and make available the contact information for such agent through its service and through the U.S. Copyright Office. The specifics for designation of such agent are set forth in subsection (8) below.

Several cases have interpreted and adjudicated the scope of the Section 512(c) safe harbor:

**a. The ALS Scan Case – What Constitutes a
“Substantially” Compliant Notice**

The issue of what constitutes a “substantially” compliant notice under Section 512(c)(3) was addressed in the case of ALS Scan, Inc. v. RemarQ Communities, Inc.³¹⁴⁰ In that case, the defendant RemarQ was an OSP that provided access to its members to over 30,000 newsgroups. RemarQ did not monitor, regulate, or censor the content of articles posted in the newsgroups, but did have the ability to filter information contained in the newsgroups and to screen its members from logging onto certain newsgroups, such as those containing pornographic material.³¹⁴¹ The plaintiff ALS Scan, Inc. (ALS Scan) was in the business of creating and marketing “adult” photographs. The plaintiff discovered that two newsgroups on the RemarQ service – both of which had “als” in their titles (alt.als and alt.binaries.pictures.erotica.als) – contained virtually nothing other than unauthorized photographs owned by ALS Scan. ALS Scan sent a cease and desist letter to RemarQ, demanding that RemarQ block access to both of the newsgroups at issue.³¹⁴²

RemarQ responded by refusing to comply with ALS Scan’s demand but advising ALS Scan that RemarQ would eliminate individual infringing items from the newsgroups if ALS Scan identified them “with sufficient specificity.”³¹⁴³ ALS Scan filed suit, alleging copyright infringement and violations of Title II of the DMCA. In response, RemarQ filed a motion to dismiss the complaint or, in the alternative, for summary judgment, and attached affidavits stating that it was prepared to remove articles posted in its newsgroups if the allegedly infringing articles were specifically identified as required by the DMCA. The district court dismissed the complaint, ruling that RemarQ could not be liable for contributory infringement because ALS Scan failed to comply with the notice requirements of Section 512(c)(3)(A) of the DMCA.³¹⁴⁴

³¹⁴⁰ 239 F.3d 619 (4th Cir. 2001).

³¹⁴¹ Id. at 620.

³¹⁴² Id.

³¹⁴³ Id. at 621.

³¹⁴⁴ Id.

On appeal, ALS Scan contended that it “substantially” complied with the notice requirements of the DMCA and that it therefore put RemarQ sufficiently on notice of infringement activities that RemarQ lost its immunity under the DMCA by failing to remove the infringing material. RemarQ argued in response that it did not have knowledge of the infringing activity as a matter of law because ALS Scan failed to identify the infringing works as required by the DMCA, and RemarQ was entitled to the safe harbor provisions of the DMCA.³¹⁴⁵

The Fourth Circuit reversed on two grounds. First, the court noted that, in order to be entitled to the safe harbor of Section 512(c), an OSP must satisfy all three of the safe harbor requirements of Section 512(c)(1), specifically, that: (i) it has neither actual knowledge that its system contains infringing materials nor awareness of facts or circumstances from which infringement is apparent, or it has expeditiously removed or disabled access to infringing material upon obtaining actual knowledge of infringement; (ii) it receives no financial benefit directly attributable to infringing activity; and (iii) it responded expeditiously to remove or disable access to material claimed to be infringing after receiving notice from the copyright holder conforming to the requirements of Section 512(c)(3). The Fourth Circuit held that “a showing under the first prong – the lack of actual or constructive knowledge – is prior to and separate from the showings that must be made under the second and third prongs.”³¹⁴⁶ The Fourth Circuit noted that, although it had treated RemarQ’s motion as a motion to dismiss, rather than as a motion for summary judgment, it had failed to take into account the allegation in the complaint that RemarQ had actual knowledge of the infringing nature of the two newsgroups even before being contacted by ALS Scan. Although this allegation was denied by RemarQ, the Fourth Circuit noted that the district court was required to accept the allegation as true for purposes of testing the adequacy of the complaint under F.R.C.P. 12(b)(6).³¹⁴⁷

Second, whether or not RemarQ’s motion was treated as one to dismiss or for summary judgment, the Fourth Circuit held that ALS Scan had substantially complied with the notice requirement of the third prong. The district court had found that ALS Scan’s notice failed to comply with two of the six requirements of notification – namely, that the notice include a list of infringing works on the RemarQ site and that the notice identify the infringing works in sufficient detail to enable RemarQ to locate and disable them (per Section 512(c)(3)(A)(ii) & (iii)).³¹⁴⁸

The Fourth Circuit disagreed, noting that under Section 512(c)(3)(A), a notice need comply with the prescribed format only “substantially,” and under Section 512(c)(3)(A)(ii), a copyright holder need only provide a “representative” list of infringed works on the site.³¹⁴⁹ The court stated: “This subsection specifying the requirements of a notification does not seek to burden copyright holders with the responsibility of identifying every infringing work – or even

³¹⁴⁵ Id. at 622.

³¹⁴⁶ Id. at 623.

³¹⁴⁷ Id.

³¹⁴⁸ Id. at 621.

³¹⁴⁹ Id. at 625.

most of them – when multiple copyrights are involved. Instead, the requirements are written so as to reduce the burden of holders of multiple copyrights who face extensive infringement of their works. Thus, when a letter provides notice equivalent to a list of representative works that can be easily identified by the service provider, the notice substantially complies with the notification requirements.”³¹⁵⁰

The Fourth Circuit found that on the particular facts of the case, ALS Scan’s notice constituted an adequate representative list of infringed works and substantially complied with the DMCA notice requirements:

In this case, ALS Scan provided RemarQ with information that (1) identified two sites created for the sole purpose of publishing ALS Scan’s copyrighted works, (2) asserted that virtually all the images at the two sites were its copyrighted material, and (3) referred RemarQ to two web addresses where RemarQ could find pictures of ALS Scan’s models³¹⁵¹ and obtain ALS Scan’s copyright information. In addition, it noted that material at the site could be identified as ALS Scan’s material because the material included ALS Scan’s ‘name and/or copyright symbol next to it.’ We believe that with this information, ALS Scan substantially complied with the notification requirement of providing a representative list of infringing material as well as information reasonably sufficient to enable RemarQ to locate the infringing material.³¹⁵²

Because RemarQ had received adequate notice of infringement and had failed to act to remove the infringing material, it was not entitled to the safe harbor of the DMCA.³¹⁵³ The Fourth Circuit observed that the immunity of the DMCA “is not presumptive, but granted only to ‘innocent’ service providers who can prove they do not have actual or constructive knowledge of the infringement, as defined under any of the three prongs of 17 U.S.C. § 512(c)(1). The DMCA’s protection of an innocent service provider disappears at the moment the service provider loses its innocence; i.e., at the moment it becomes aware that a third party is using its system to infringe. At that point, the Act shifts responsibility to the service provider to disable the infringing material”³¹⁵⁴ The Fourth Circuit remanded the case for further proceedings on ALS

³¹⁵⁰ Id.

³¹⁵¹ It is curious that the Fourth Circuit found the supplied Web address where RemarQ could find pictures of ALS Scan’s models to aid ALS Scan’s argument that RemarQ had adequate notice of what particular infringing photographs were contained on RemarQ’s site. The referenced Web address contained adult “teaser” photos of the ALS Scan models. There is nothing in the opinion of the court indicating that the “teaser” photos were the actual ones allegedly on the RemarQ site. Rather, the argument seems to be that the “teaser” photos would identify what the ALS Scan models looked like. Is the Fourth Circuit implying that RemarQ then bore the burden to go look at the photos on the newsgroups at issue to see if they contained pictures of the same humans as those in the “teaser” photos? Perhaps the truly key facts were that the infringing photos in the newsgroups were identified with ALS Scan’s name and/or copyright notice and they were all contained in one “place” – namely, a couple of particular newsgroups almost entirely devoted to ALS Scan photos.

³¹⁵² Id.

³¹⁵³ Id. at 625-26.

³¹⁵⁴ Id. at 625.

Scan's copyright infringement claims and any other affirmative defenses that RemarQ might have.³¹⁵⁵

There are a few lessons to be learned from the ALS Scan case. First, where multiple copyrighted works are allegedly infringed, a copyright holder need not specifically identify all particular instances of infringing material at the site in order to give adequate notice to the Service Provider sufficient to give rise to a duty on its part to act in order to preserve the DMCA safe harbors. Second, at least in the specific factual scenario where all the allegedly infringing material is contained in a single area such as a newsgroup, and the area comprises almost all infringing material, the Service Provider may need to remove or block access to the entire area as a precaution to preserve the safe harbor. It might have been sufficient for RemarQ to have removed or blocked access only to those photos within the newsgroups that bore ALS Scan's name or copyright notice (the opinion does not address this question) – but even if so, it appears that the Fourth Circuit may have contemplated that RemarQ, and not ALS Scan, would bear the burden of identifying the individual photos for removal or blocking access to. Third, the decision suggests that a Service Provider may not be wise to rely on certain failures on the part of a copyright holder to comply with all the technical notice requirements of Section 512(c)(3) as a basis for not having to act to remove or block allegedly infringing material. If a court later determines that the notice was “substantially” compliant, the Service Provider may have lost its DMCA safe harbor by failing to act.

In sum, the ALS Scan case reflected a rather low threshold of knowledge of infringing activity, at least under the specific facts of the case, and a rather lax application of the technical notice requirements of Section 512(c). The net effect of these rulings was to make the Section 512(c) safe harbor rather fragile for the OSP. Subsequent cases have given the Section 512(c) safe harbor a stronger reading in favor of the OSP and have insisted on a stricter compliance with the technical notice requirements on the part of the copyright holder:

b. Hendrickson v. eBay

In Hendrickson v. eBay Inc.,³¹⁵⁶ the plaintiff Hendrickson, a pro se plaintiff, sought to hold defendant eBay Inc. secondarily liable for the sale through the eBay auction site of allegedly infringing copies of the documentary film “Manson” in DVD format. The plaintiff sent a cease and desist letter to eBay, which stated generally that pirated copies of “Manson” were being offered for sale on eBay, but did not explain which copies of “Manson” were infringing, nor did it identify the plaintiff's copyright interest. eBay responded by requesting that the plaintiff comply with the notice requirements of Section 512(c), and suggesting that the plaintiff submit a copy of eBay's “Notice of Infringement” form, which would comply with the notice requirements of the DMCA and would specify which particular item numbers (each listing on eBay's site had its own item number) were infringing so eBay could remove them. The plaintiff refused to submit the

³¹⁵⁵ Id. at 626.

³¹⁵⁶ 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

Notice of Infringement form or otherwise specify which particular items on eBay were allegedly infringing, and instead filed a copyright infringement lawsuit.³¹⁵⁷

eBay asserted the safe harbor of Section 512(c) as a defense. The court began its analysis by noting that there was no dispute over whether eBay qualified as a “service provider” within the meaning of Section 512(k)(1)(B).³¹⁵⁸ The court noted that Section 512(c) was the appropriate safe harbor potentially applicable to eBay because that safe harbor applies to infringing “activity using the material on” an OSP’s system.³¹⁵⁹

The court then turned to an analysis of the issue of proper notice of infringement. Under Section 512(c)(1)(C), a service provider’s duty to act to remove material that is the subject of infringing activity is “triggered only upon receipt of proper notice” substantially compliant with the required elements of notification set forth in Section 512(c)(3).³¹⁶⁰ As a preliminary matter, the court rejected the plaintiff’s argument that he need not submit written notification in compliance with the notice requirements of Section 512(c)(3) “as long as other facts show the service provider received actual or constructive knowledge of infringing activity.”³¹⁶¹ The court replied that, under Section 512(c)(3)(B)(i), if the copyright holder’s attempted notification fails to comply substantially with the elements of Section 512(c)(3), then the notification cannot be considered when evaluating whether the service provider had actual or constructive knowledge of the infringing activity.³¹⁶²

Because the plaintiff admitted that he had not strictly complied with the notice requirements of Section 512(c)(3), the court turned to an analysis of whether his imperfect attempt to give notice constituted “substantial” compliance, and ruled that it did not because his notice did not include several key elements for proper notification:

- There was no written statement attesting under penalty of perjury that the information in the notification was accurate and that the plaintiff was authorized to act on behalf of the copyright owner, or that the plaintiff had a good faith belief that use of the material in the manner complained of was not authorized. The court held that the plaintiff’s complete failure to supply the preceding two elements, even after eBay specifically asked for them, rendered the plaintiff’s notification of claimed infringement deficient under Section 512(c)(3).³¹⁶³

- There was not sufficient information to identify the various listings on eBay that purportedly offered pirated copies of “Manson,” and the plaintiff had refused to supply such

³¹⁵⁷ Id. at 1084-85.

³¹⁵⁸ Id. at 1088.

³¹⁵⁹ Id. (quoting 17 U.S.C. § 512(c)(1)(A)(i)).

³¹⁶⁰ 165 F. Supp. 2d at 1089.

³¹⁶¹ Id.

³¹⁶² Id.

³¹⁶³ Id. at 1089-90.

information when specifically asked by eBay.³¹⁶⁴ The plaintiff contended that it was “not his job to do so once he has notified eBay of the existence of infringing activity by eBay sellers.”³¹⁶⁵ The court rejected this argument, stating: “The Court recognizes that there may be instances where a copyright holder need not provide eBay with specific item numbers to satisfy the identification requirement. For example, if a movie studio advised eBay that all listings offering to sell a new movie (*e.g.*, ‘Planet X,’) that has not yet been released in VHS or DVD format are unlawful, eBay could easily search its website using the title ‘Planet X’ and identify the offensive listings. However, the record in this case indicates that specific item numbers were necessary to enable eBay to identify problematic listings.”³¹⁶⁶

– There was no written statement to eBay that all DVD copies of “Manson” were unauthorized copies. Although the plaintiff stated at oral argument that he had orally notified eBay that all copies of “Manson” in DVD format were unauthorized, this was insufficient because it was not in writing. “The writing requirement is not one of the elements listed under the substantial compliance category [of Section 512(c)(3)(A).] Therefore, the Court disregards all evidence that purports to show Plaintiff gave notice that all DVDs violate his copyright in ‘Manson.’”³¹⁶⁷

The court rejected two other arguments offered by the plaintiff concerning why he should not be required to supply eBay with specific item numbers of allegedly infringing copies. First, he argued that he had supplied eBay with user IDs of four alleged infringers, and the user IDs should be sufficient notice to locate the listings offering pirated copies of “Manson.” The court ruled the notice of user IDs insufficient because the email containing the user IDs did not identify either the listings claimed to be the subject of infringing activity or describe the infringing activity, nor did it contain a statement attesting to the good faith and accuracy of the allegations.³¹⁶⁸ Second, the plaintiff argued that eBay could identify listings offering infringing copies without item numbers because eBay had previously removed two listings even though the plaintiff did not provide the item numbers. The court rejected this argument also, noting that the plaintiff had identified one of the sellers that eBay removed, who because it had only a single listing at the time of removal, eBay had removed out of an abundance of caution, and the record did not reflect why eBay removed the second listing.³¹⁶⁹

In sum, the court ruled that proper identification under Section 512(c)(3)(A)(iii) should include the item numbers of the listings that were allegedly offering pirated copies of

³¹⁶⁴ Id. at 1090.

³¹⁶⁵ Id.

³¹⁶⁶ Id.

³¹⁶⁷ Id. at 1091. Similarly, noting Plaintiff’s admission that authorized copies of “Manson” had been released in VHS format, the Court ruled that the plaintiff had offered no explanation to eBay how it could determine which “Manson” VHS tapes being offered for sale were unauthorized copies. Id.

³¹⁶⁸ Id.

³¹⁶⁹ Id. at 1091-92.

“Manson.”³¹⁷⁰ Because the plaintiff had failed to submit a written notice substantially complying with the notice requirements of Section 512(c), eBay did not have a duty to act under Section 512(c)(1)(C) to remove the allegedly infringing listings, and would therefore be entitled to the Section 512(c) safe harbor if it met the remaining prongs of the safe harbor test.³¹⁷¹

– Absence of Actual or Constructive Notice: Because the plaintiff’s notices did not substantially comply with the notice requirements of Section 512(c), the court ruled that they could not, as a matter of law, establish actual or constructive knowledge that particular listings were involved in infringing activity. Since the record showed that eBay otherwise did not have actual or constructive knowledge before the lawsuit was filed, the court ruled that eBay had satisfied the first prong of the safe harbor test under Section 512(c)(1)(A).³¹⁷²

– Right and Ability to Control the Infringing Activity: Under Section 512(c)(1)(B), eBay was required to show that it did not receive a financial benefit directly attributable to the infringing activity in a case in which it had the right and ability to control such activity. The court ruled that, because the undisputed facts established that eBay did not have the right and ability to control the infringing activity, the court need not evaluate the financial benefit element.³¹⁷³ Plaintiff argued that eBay had the ability to control infringing activity based on its ability to remove infringing listings after receiving proper notification, and its program of prophylactic searching for apparent infringements based on searching its website daily for generic key words such as “bootleg,” “pirated,” “counterfeit” and “taped off TV” that might indicate potentially infringing activity.³¹⁷⁴ The court rejected these arguments, first noting the Catch 22 that would arise if the mere ability to remove infringing materials were sufficient to satisfy the control prong, since the DMCA requires an OSP to remove infringing materials:

[T]he ‘right and ability to control’ the infringing activity, as the concept is used in the DMCA, cannot simply mean the ability of a service provider to remove or block access to materials posted on its website or stored in its system. To hold otherwise would defeat the purpose of the DMCA and render the statute internally inconsistent. The DMCA specifically requires a service provider to remove or block access to materials posted on its system when it receives notice of claimed infringement. The DMCA also provides that the limitations on liability *only* apply to a service provider that has ‘adopted and reasonably implemented ... a policy that provides for the termination in appropriate circumstances of [users] of the service provider’s system or network who are repeat infringers.’ Congress could not have intended for courts to hold that a service provider

³¹⁷⁰ Id. at 1092.

³¹⁷¹ Id.

³¹⁷² Id. at 1093.

³¹⁷³ Id.

³¹⁷⁴ Id. at 1093 & n. 14.

loses immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically required by the DMCA.”³¹⁷⁵

Nor could eBay’s voluntary practice of engaging in limited monitoring of its website for apparent infringements satisfy the control prong. The court cited a passage of the legislative history of the DMCA stating that courts “should not conclude that the service provider loses eligibility for limitations on liability under section 512 solely because it engaged in a monitoring program.”³¹⁷⁶ Finally, the court noted that the infringing activity actually took place offline in the form of the sales and distribution of pirated copies of “Manson,” and that eBay could not control such offline activity.³¹⁷⁷

The court concluded that eBay had established that it met the test for the safe harbor under Section 512(c), and accordingly granted eBay summary judgment on the plaintiff’s copyright claims.³¹⁷⁸

Important Principles. The Hendrickson v. eBay case establishes a number of significant points about the Section 512(c) safe harbor. First, insofar as the OSP receives notice of alleged infringement on its system from the *copyright holder*, such notice must be in writing and must substantially comply with the technical notice requirements of Section 512(c). The OSP can, of course, receive actual or constructive notice through channels other than the copyright holder, but notice from the copyright holder must come in written form in order to trigger the OSP’s duty to act on that information. The ALS Scan case is consistent on this point, since in the ALS Scan case, notice from the copyright holder was in writing. Second, the copyright holder bears the burden to identify specific instances of infringing activity on the system. It is insufficient to identify only the users who are committing allegedly infringing acts without further identification of the infringing *materials* that are the subject of those acts. Third, neither the OSP’s mere ability to terminate infringing users or activity, or the OSP’s voluntary policing of its system or website, will of themselves be sufficient to establish “control” of the infringing activity for purposes of adjudicating the availability of the Section 512(c) defense.

c. CoStar v. LoopNet

³¹⁷⁵ Id. at 1093 (citations omitted).

³¹⁷⁶ Id. at 1094 (quoting House Report 105-796 at 73 (Oct. 8, 1998)).

³¹⁷⁷ 165 F. Supp. 2d at 1094. This is an interesting holding, since removing the listing from eBay’s service would have had the derivative effect of controlling the ability of users to make offline purchases and distributions in the first place. The same rationale would seem to apply to the Napster service, in which Napster could not control whether its users elected to make downloads of allegedly infringing materials posted on the Napster index, which downloads did not pass through the Napster servers. Notwithstanding this fact, the district court in the Napster case, as discussed above, found that Napster did in fact have sufficient “control” over the infringing activity by virtue of its control over the listings in the Napster index.

³¹⁷⁸ Id. The court also held that eBay’s immunity under the safe harbor extended to the plaintiff’s claims against eBay employees. Id. at 1094-95.

In CoStar Group Inc. v. LoopNet, Inc.,³¹⁷⁹ the plaintiff CoStar maintained a copyrighted commercial real estate database that included photographs. The defendant LoopNet offered a service through which a user, usually a real estate broker, could post a listing of commercial real estate available for lease. The user would access, fill out, and submit a form for the property available. To include a photograph of the property, the user was required to fill out another form. The photograph would initially be uploaded into a separate folder on LoopNet's system, where it would first be reviewed by a LoopNet employee to determine that it was in fact a photograph of commercial property and that there was no obvious indication the photograph was submitted in violation of LoopNet's terms and conditions. If the photograph met LoopNet's criteria, the employee would accept it and post it along with the property listing. CoStar claimed that over 300 of its copyrighted photographs had been posted on LoopNet's site, and sued LoopNet for both direct and contributory copyright liability.³¹⁸⁰ The court entered a preliminary injunction against LoopNet. CoStar then moved for summary judgment on LoopNet's liability, and LoopNet moved for summary judgment on noninfringement and its entitlement to the safe harbor of Section 512(c).

CoStar argued that LoopNet should be directly liable for copyright infringement because, acting through its employees' review and subsequent posting of the photographs, LoopNet was directly copying and distributing the photographs, citing the Frena case discussed above in Section II.A.4(d). The court rejected this argument, noting that the Fourth Circuit in the ALS Scan case had concluded that the legislative history of the DMCA indicated Congress' intent to overrule the Frena case and to follow the Netcom case, under which an OSP's liability for postings by its users must be judged under the contributory infringement doctrine.³¹⁸¹

The court then turned to an analysis of contributory infringement and the safe harbor of Section 512(c) of the DMCA asserted by LoopNet. CoStar argued, citing the Fonovisa "swap meet" case³¹⁸² that was relied on by the Ninth Circuit in the Napster I case,³¹⁸³ that once it had given LoopNet notice of specific alleged infringements, LoopNet had sufficient knowledge of ongoing infringements by its users to be liable for contributory infringement based on its failure to take more "drastic measures" to prevent infringement.³¹⁸⁴ LoopNet argued that it could not be liable for contributory infringement because it had no knowledge of the infringements prior to notice from CoStar, and it discontinued access to the infringing material immediately upon discovery. LoopNet also argued that its DMCA policy for removal of infringing material and of

³¹⁷⁹ 164 F. Supp. 2d 688 (D. Md. 2001), aff'd, 373 F.3d 544 (4th Cir. 2004).

³¹⁸⁰ Id. at 691-92.

³¹⁸¹ Id. at 695-96.

³¹⁸² Fonovisa v. Cherry Auction, 76 F.3d 259 (9th Cir. 1996).

³¹⁸³ A&M Records v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

³¹⁸⁴ CoStar, 164 F. Supp. 2d at 696-97.

denying access to repeat infringers was sufficient both to give it the benefit of the Section 512(c) safe harbor and to avoid common law contributory liability.³¹⁸⁵

Turning first to the issue of knowledge, the court held that LoopNet did not have knowledge of the alleged infringements prior to receiving notice from CoStar, based on the facts that CoStar did not attach copyright notices to its photographs and LoopNet did not know what rights CoStar may have granted in license agreements to users of its commercial real estate database containing the photographs.³¹⁸⁶ Citing the Netcom case, the court ruled, “In the case of a service provider, knowledge giving rise to liability only exists when there is no colorable claim of users’ noninfringement.”³¹⁸⁷ LoopNet could therefore not be charged with any form of knowledge before receiving claims of infringement from CoStar. The central issue, then, was whether LoopNet’s policies to deter infringement, remove infringing works, and prevent repeat infringement were adequate both under the common law and for purposes of the DMCA safe harbor.³¹⁸⁸ In an important ruling, the court held that the parameters of the liability protection provided by the Section 512(c) safe harbor were “not contiguous with the bounds of liability for contributory infringement.”³¹⁸⁹ This is contrary to the opposite conclusion reached by the district court in an early decision in the Napster case,³¹⁹⁰ later reversed by the Ninth Circuit,³¹⁹¹ that the parameters for safe harbor liability protection and common law contributory liability were contiguous, and the safe harbor could therefore not protect contributory infringers.

The court then turned to a detailed analysis of whether CoStar was entitled to the benefit of the Section 512(c) safe harbor. As a threshold matter, the court held that the definition of “service provider” under Section 512(k)(1)(B) was broad and easily encompassed the type of service provided by LoopNet.³¹⁹² The court also ruled that the safe harbor could not protect LoopNet for any alleged infringements taking place before December 8, 1999, the date that LoopNet designated an agent to receive notifications of claimed infringement under the DMCA,

³¹⁸⁵ Id. at 697-98.

³¹⁸⁶ Id. at 698. The court further noted that the fact that CoStar’s employees were involved in manually examining photographs before they were posted on the site did not change the knowledge analysis. “LoopNet has people checking photographs for purposes other than copyright infringement and CoStar’s own experts could not distinguish between a CoStar and non-CoStar photograph upon inspection.” Id. at 700 n. 6.

³¹⁸⁷ Id. at 698. This is a rather high standard for knowledge for contributory infringement – it seems that in the many circumstances in which an OSP does not have any direct involvement with its users’ postings of materials on its site, the OSP will be unable to be certain that there is “no colorable claim” of its users’ noninfringement.

³¹⁸⁸ Id. at 698-99.

³¹⁸⁹ Id. at 699.

³¹⁹⁰ A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 919 n. 24 (N.D. Cal. 2000).

³¹⁹¹ A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025 (9th Cir. 2001).

³¹⁹² CoStar, 164 F. Supp. 2d at 701.

as required by Section 512(c)(2) of the DMCA.³¹⁹³ The court then turned to an analysis of several specific issues under the safe harbor.

Storage at the Instance of the User. CoStar argued that the Section 512(c) safe harbor should not apply at all because the allegedly infringing photographs were uploaded to the site only after review and selection by LoopNet and so were not stored at the instance of LoopNet's users. The court rejected this argument, reasoning that the photographs were uploaded at the volition of the LoopNet users and that LoopNet subjected them only to a gateway screening process, not a selection process. The court also held that the mere ability to remove or block access to materials could not mean that those materials were not stored at the user's discretion. Noting that Section 512 mandates a "take down" procedure to qualify for the Section 512(c) safe harbor, the court held that it would be internally illogical if the statute were construed to mean that in order to get into the safe harbor, an OSP needed to lack control to remove or block access.³¹⁹⁴

Knowledge for Purposes of the Safe Harbor. Turning to the issue of knowledge, the court noted that three types of knowledge could take a service provider outside the safe harbor: (i) actual knowledge; (2) awareness of facts raising a "red flag" that its users are infringing; and (iii) notification from the copyright holder in compliance with the technical notice requirements of Section 512(c)(3). The court noted that a service provider does not automatically lose the safe harbor upon receiving notice, but the DMCA shifts responsibility to the service provider to disable the infringing material.³¹⁹⁵ Specifically, "[i]f the service provider has actual knowledge under § 512(c)(1)(A)(i) or 'red flag' knowledge under § 512(c)(1)(A)(ii), the 'take down' provisions of § 512(c)(1)(A)(iii) must be met to stay in the safe harbor. Alternatively, if it receives notification of claimed infringement in accordance with § 512(c)(3), the 'take down' provisions of § 512(c)(1)(C) must be met."³¹⁹⁶

Because LoopNet had not challenged the adequacy of notification it had received from CoStar, the court turned to the adequacy of LoopNet's removal policy. The court noted that LoopNet had two responsibilities after receipt of notice from the copyright holder:³¹⁹⁷ First, under Section 512(c)(1)(C), it must respond "expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity." Second, under Section 512(i)(1)(A), it must adopt and reasonably implement, and inform subscribers of, a policy "that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."

³¹⁹³ Id. at 697 & n.4.

³¹⁹⁴ Id. at 701-02.

³¹⁹⁵ Id. at 702.

³¹⁹⁶ Id. at 702 n. 8.

³¹⁹⁷ Id. at 703.

The court ruled that factual issues on each of these two issues precluded summary judgment: CoStar claimed that LoopNet had failed to remove several photographs after being notified that they were infringing and that several photographs had been posted more than once after notification. CoStar also alleged that there was no evidence LoopNet had ever terminated any user's access despite the fact that some of them had an extensive history as repeat infringers.³¹⁹⁸ LoopNet countered that its "Terms and Conditions" for its site included the removal of listings alleged to be infringing and the possibility of termination. LoopNet also claimed that it promptly removed photographs once it received notice of alleged infringement, sent an email to brokers explaining the potential consequences of repeat infringement and investigated brokers it suspected to be repeat infringers. It also claimed to have implemented additional precautions to avoid reposting of infringing photographs in the future. In addition, the court noted that because LoopNet's take down and termination policies had changed over time, to resolve the issue of the adequacy of those procedures, a factfinder would have to focus on each photograph alleged to be infringing and the policy in effect before the posting of each photograph.³¹⁹⁹

Financial Benefit. To begin its analysis of the financial benefit prong of the Section 512(c) safe harbor, the court, in a significant ruling, noted that, "[r]egardless of whether LoopNet complied with the 'take down' requirements, a finding that it received a direct financial benefit from the infringement automatically would remove it from the safe harbor. ... Basically, the DMCA provides no safe harbor for vicarious infringement because it codifies both elements of vicarious liability."³²⁰⁰ The ruling that the DMCA provides no safe harbor for vicarious infringement seems to contradict the Ninth Circuit's ruling in the Napster I case, discussed in the next subsection, in which the Ninth Circuit noted that "[w]e do not agree [with the district court's ruling] that Napster's potential liability for contributory and vicarious infringement renders the Digital Millennium Copyright Act inapplicable per se."³²⁰¹

The court held that LoopNet did not meet either element of the test for vicarious liability. CoStar had not asserted that LoopNet had any right to control its users beyond its mere ability to control or block access to its site. The court, citing the Hendrickson v. eBay case, held that such ability to block access could not constitute sufficient "right and ability" to control for vicarious liability. The court noted that otherwise one would have the illogical result that the very policy of blocking access and terminating infringers mandated by the DMCA in Section 512(c)(1)(C) would force service providers to lose their immunity by violating § 512(c)(1)(B).³²⁰² The court also ruled that LoopNet did not receive a direct financial benefit from the infringing activity

³¹⁹⁸ Id.

³¹⁹⁹ Id. at 703-04.

³²⁰⁰ Id. at 704 (citing 3 M. Nimmer & D. Nimmer, Nimmer on Copyright, § 12B.04[A][2], at 12B-38 (2001)).

³²⁰¹ A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025 (9th Cir. 2001).

³²⁰² CoStar, 164 F. Supp. 2d at 704 & n.9.

because LoopNet did not charge a fee for posting any real estate listing, with or without a photograph.³²⁰³

Contributory Liability Before the Safe Harbor Applicability Date. The court next turned to an analysis of LoopNet's contributory liability for activity before December 8, 1999, the date that LoopNet designated an agent to receive notifications of claimed infringement under the DMCA and therefore first became eligible for the Section 512(c) safe harbor. The court's discussion of common law liability provides a nice analysis of the interplay and differences between the standards of knowledge and policing for infringing activity required under the common law versus the DMCA safe harbors.

Knowledge for Purposes of Common Law Liability. CoStar argued that once it gave LoopNet notice of specific infringements, LoopNet was on notice that ongoing infringements were occurring and had a duty to prevent repeat infringements. LoopNet argued that it could not be charged with imputed knowledge of future infringements. The court held that the amount of policing for future infringements LoopNet would be required to do would depend upon the level of knowledge it possessed:

There is a critical interplay between the level of knowledge possessed by LoopNet as a result of CoStar's notices and the amount of policing, deterrence and removal demanded of LoopNet to avoid being liable for contributory infringement. If CoStar's notice to LoopNet gave LoopNet a broad scope of knowledge that infringements were occurring, then it creates a high level of policing necessary by LoopNet to avoid inducing infringement.

The issue of the adequacy of LoopNet's removal policy is different at this stage than it was when assessing its adequacy for the purposes of the DMCA safe harbor. In the safe harbor context, the removal policy had adequately to remove infringing or allegedly infringing material. If LoopNet met the standard following notice it was shielded from damages liability by the safe harbor. In the context of assessing liability for contributory infringement, the question is not whether LoopNet adequately removed the infringing material, but whether, at some point, it created an inducement to put infringing material up on the site.³²⁰⁴

The court noted that, while LoopNet's continued control over access to its site made it more similar to the swap meet owner in the Fonovisa case or the BBS operator in the Maphia case than to the mere seller of goods in the Sony case, there were elements of knowledge in the Fonovisa and Maphia cases that the court found not present in the instant case. Instead, the court analogized to the Netcom case, finding that LoopNet's circumstances resided "in that gray middle range of cases in which the service provider has information suggesting, but not conclusively demonstrating, that subscribers committed infringement. ... Netcom stands for the

³²⁰³ Id. at 704.

³²⁰⁴ Id. at 706.

proposition that the bare claim of infringement by a copyright holder does not necessarily give rise to knowledge of an infringement.”³²⁰⁵

The court contrasted LoopNet’s situation from the Napster and Fonovisa cases, where the defendant had actual, specific knowledge of infringements and continued to provide support and facilities to infringers. “Thus, in order to prove its claim, CoStar needs to establish that the notice it gave to LoopNet comprised at least constructive knowledge of specific infringing activity which LoopNet materially contributed to or induced by its alleged failure to halt the activity. There remain too many material factual disputes for the court to decide on summary judgment either that such a level of knowledge did or did not exist or that LoopNet’s actions in trying to stop the infringement were or were not insufficient to the point of comprising inducement as a matter of law.”³²⁰⁶ Accordingly, the court denied summary judgment on the issue of common law contributory liability.³²⁰⁷

Statutory Damage Award. CoStar elected to take a statutory damages award under Section 504(c)(1) of the copyright statute, which provides that the copyright owner may elect to take statutory damages in lieu of actual damages and profits for “all infringements involved in the action, with respect to any one work ...” The court turned to the issue of what constitutes a “work” for purposes of statutory damages. LoopNet argued that CoStar was limited to no more than 13 statutory damages awards because it had only 13 copyright registrations (the photographs had been registered in groups as compilations). CoStar argued that each of its 348 photographs constituted a separate work and, therefore, it was entitled to 348 separate statutory damages awards.³²⁰⁸

The court noted a division of authority over whether the copyright registration is determinative of the number of works or whether the determinative factor is whether each work is independently copyrightable. After reviewing the facts of various cases, the court concluded that the critical fact was “not that CoStar registered multiple photographs on the same registration form, but whether it registered them as compilations or as individual copyrights.”³²⁰⁹ The court noted that the language on the registration application under “Nature of Authorship”

³²⁰⁵ Id. at 707. The court further observed: “In the analysis of LoopNet’s safe harbor defense to liability, mere notification of claimed infringement by CoStar was enough to trigger one of two scenarios. Either LoopNet could comply with the ‘take-down’ provisions of the DMCA and remain in the safe harbor or refuse to remove the allegedly infringing material and expose itself to the choppy waters of contributory infringement liability.” Id.

³²⁰⁶ Id. at 707-08.

³²⁰⁷ LoopNet raised a misuse defense, arguing that CoStar had misused its copyrights in the photographs by extending them beyond their intended reach to limit its licensees from distributing the entire database, including data and photographs in which it had no copyright. Id. at 708. The court rejected this defense with relatively little analysis, distinguishing other copyright misuse cases factually and concluding “there is no allegation or tying or abuse of copyright serious enough to offend the public policy behind copyright and rise to the level of misuse.” Id. at 709.

³²⁰⁸ Id.

³²⁰⁹ Id. at 711.

on all but the first registration read “revised compilation of database information; some original text and photographs.”³²¹⁰ The first registration read “compilation, text, and photographs,” but under the description of the work to be registered, the form read “compilation of public domain material, substantial original text, and original photographs.”³²¹¹ The court concluded that the preceding language indicated that all of the registrations were compilation registrations, because the reference to “photographs” could only have efficacy as a description of the work to be registered if it was made with reference to the other elements being copyrighted – the compilation of work.³²¹² Accordingly, CoStar was eligible for only 13 statutory damage awards, corresponding to the number of registered compilations.³²¹³

The Scope of the Preliminary Injunction. An interesting aspect of the case concerned the scope of preliminary injunction the court entered against LoopNet and the obligations the court imposed on LoopNet once it was notified that one of its users had posted an infringing photograph on the LoopNet system. In an earlier proceeding, the court had entered a preliminary injunction directing LoopNet to “(1) remove from its web site all photographs for which it received notification of claimed infringement from CoStar; (2) notify the user who uploaded the photograph of CoStar’s claim of the removal and that repeat acts of infringement might result in restrictions on the user’s (or the brokerage firm’s) access to the web site; and (3) with regard to identified brokers, require *prima facie* evidence of copyright ownership prior to posting a photograph.”³²¹⁴ Dissatisfied with LoopNet’s performance, CoStar sought a number of substantial modifications to the requirements imposed on LoopNet, including a requirement to obtain a hand-signed written declaration of copyright ownership prior to any posting and a requirement that any repeat infringer thereafter be prohibited from submitting any further photographs.³²¹⁵

The court refused to make the modifications requested by CoStar. In view of its rulings with respect to the contributory infringement and safe harbor issues, the court concluded that CoStar had not shown a sufficient likelihood of success to justify the enhancements to the order it sought.³²¹⁶ The court did, however, rule that a probation/termination policy LoopNet had set up, in which brokers who posted infringing photographs could have their probationary status removed in three, six, or twelve month intervals, was inadequate in two respects: “First, all brokers in an office in which any broker posted an allegedly infringing photograph after notice to any broker in that same office should be subject to the *prima facie* evidence requirement.”³²¹⁷

³²¹⁰ Id.

³²¹¹ Id.

³²¹² Id. at 711-12.

³²¹³ Id. at 712.

³²¹⁴ Id. at 715.

³²¹⁵ Id. at 715-16.

³²¹⁶ Id. at 716.

³²¹⁷ Id.

Second, the court required that the status of “repeat infringer,” once achieved, remain during the pendency of the proceedings, with no possibility of discontinuing such status after a time interval.³²¹⁸

Subsequent to the district court’s rulings, the parties stipulated to the dismissal of all claims except the district court’s summary judgment in favor of LoopNet on direct infringement, and CoStar appealed.³²¹⁹ The Fourth Circuit’s rulings with respect to the issue of direct infringement are discussed in Section II.A.4(i) above. With respect to the safe harbors, CoStar argued on appeal that Congress intended the DMCA safe harbors to supplant the common law immunity of the Netcom case, and LoopNet could therefore rely solely on the safe harbors for immunity. The Fourth Circuit rejected this argument, noting that the statute expressly states in Section 512(l) that the failure to qualify for limitation of liability under the safe harbors does not bear adversely upon the consideration of other defenses, including a defense that conduct simply does not constitute a prima facie case of infringement.³²²⁰ The court also rejected CoStar’s argument that, because Congress codified Netcom in the DMCA, it can be only to the DMCA that a defendant can look for enforcement of the principles Netcom embodied. “When Congress codifies a common-law principle, the common law remains not only good law, but a valuable touchstone for interpreting the statute, unless Congress explicitly states that it *intends* to supplant the common law.”³²²¹ The court found it clear that Congress intended the safe harbors to be a floor, not a ceiling, of protection, and the common law principles of Netcom are therefore still good law.³²²²

Important Principles. The decisions by the district court and by the Fourth Circuit in the CoStar case contain a number of important principles. First, some gateway screening of posted material by an OSP will not necessarily establish sufficient knowledge or control over allegedly infringing works to destroy the potential availability of the Section 512(c) safe harbor. Second, consistent with the Ninth Circuit’s ruling in the Napster I case discussed in subsection (iv) below, the boundaries of the contributory liability doctrine and the Section 512(c) safe harbor are not contiguous – Section 512(c) can provide a safe harbor to activity that would otherwise be infringing under the contributory liability doctrine. The CoStar case, however, reached an opposite conclusion from the Ninth Circuit in the Napster I case, as well as the Aimster/Madster and the Hendrickson v. Amazon.com cases discussed in Section III.C.6(b)(1)(i).c and Section III.C.6(b)(1)(iii).g respectively, on the issue of whether the Section 512(c) safe harbor can shield against vicarious liability (the CoStar case concluding no, the Napster I, Aimster/Madster, and Hendrickson v. Amazon.com cases concluding potentially yes).

³²¹⁸ Id. at 717.

³²¹⁹ CoStar Groups, Inc. v. LoopNet, Inc., 373 F.3d 544 (4th Cir. 2004).

³²²⁰ Id. at 552.

³²²¹ Id. at 553 (emphasis in original).

³²²² Id. at 555.

Third, consistent with the Hendrickson v. eBay case, the OSP's mere ability to terminate infringing users or activity will not of itself be sufficient to establish "control" of the infringing activity for purposes of adjudicating the availability of the Section 512(c) defense. Fourth, the amount of policing for future infringements an OSP may be required to do may depend upon the level of knowledge it possesses concerning the scope of infringing activity on its system. Although not stated as such in the Napster cases, those cases bear evidence of the principle, for the Ninth Circuit in that case imposed a heavy duty of policing in a case in which it seemed to have concluded that Napster had a substantial level of knowledge of infringing activity using its system.

d. Perfect 10 v. Cybernet Ventures

The Section 512(c) safe harbor was further adjudicated in the case of Perfect 10, Inc. v. Cybernet Ventures, Inc.,³²²³ the facts of which are set forth in Section III.C.2(f) above. Assuming that Cybernet qualified as a "provider of online services" within the definition of Section 512(k),³²²⁴ the court turned to whether Cybernet had satisfied the predicate requirements of Section 512(i) that it adopt and reasonably implement a policy providing for termination in appropriate circumstances of repeat copyright infringers. Disagreeing with the ruling of the Ellison case discussed in Section III.C.6(b)(1)(i) above, which held that Section 512(i) does not require a service provider to actually terminate repeat infringers or even to investigate infringement, but rather merely to establish a threat of termination for repeat infringement, the court in Perfect 10 v. Cybernet Ventures held that Section 512(i) does in fact imply some substantive responsibilities for service providers. Although it does not require active investigation of possible infringement, or taking action for isolated infringing acts by single users, or addressing "difficult infringement issues," or even actively monitoring for copyright infringement, the court concluded that when confronted with "appropriate circumstances," Section 512(i) requires a service provider to reasonably implement termination.³²²⁵

These circumstances would appear to cover, at a minimum, instances where a service provider is given sufficient evidence to create actual knowledge of blatant, repeat infringement by particular users, particularly infringement of a willful and commercial nature. ... Under this reading, section 512(i) is focused on infringing users, whereas 512(c) is focused primarily on the infringing material itself.³²²⁶

Analyzing the interplay between the requirements of Sections 512(i) and 512(c), the court viewed "512(i) as creating room for enforcement policies less stringent or formal than the

³²²³ 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

³²²⁴ The court noted that, although the definition is quite broad, its applicability to Cybernet was made a bit complicated by the fact that Cybernet insisted that it did not host any infringing images and that no image files passed through any of its computers, but rather that it was purely a provider of age verification services. Id. at 1175.

³²²⁵ Id. at 1176.

³²²⁶ Id. at 1177.

‘notice and take-down’ provisions of section 512(c), but still subject to 512(i)’s ‘reasonably implemented’ requirement.” The court ruled that Cybernet had not satisfied the requirements of Section 512(i). Cybernet had not submitted any documentary evidence that it had ever taken action against individual webmasters who repeatedly put up infringing sites so that such webmasters could not simply move infringing materials from site to site. Instead, Cybernet had only removed from its search engine and links page any site about which it had received a notice of infringement, without ever refusing to provide further services to the operators of those sites. Accordingly, the court concluded that Cybernet had not reasonably implemented a policy to terminate repeat infringers from its service and had therefore not satisfied the predicate requirements of Section 512(i) for the safe harbors.³²²⁷

The court further ruled that, even if Cybernet could be found to have satisfied the predicate requirements of Section 512(i), it still would not be eligible for the safe harbor of Section 512(c) for two reasons: defective implementation of notice procedures required by Section 512(c) and receipt of a direct financial benefit from infringing activity that it had a right and ability to control.

With respect to the defective implementation of notice procedures, the court noted that Cybernet’s take down policy required a complaint to comply strictly with all its stated notice requirements before Cybernet would take action, and there was no indication that Cybernet tried to work with parties whose notice was deficient but satisfied the minimal requirements of Section 512(c)(3)(B)(ii).³²²⁸ In addition, Cybernet’s notice requirements did not allow for submission of a representative list of copyrighted works being infringed – they required the specific web page at which a given infringing work was located, “rather than the site.”³²²⁹

Cybernet’s counter-notification procedures were also ruled defective. The court held that the counter-notification procedures of the DMCA implicate the requirement of a reasonably implemented Section 512(i) policy “because there is an implication that a party who cannot sign the required statement is a knowing infringer. Thus, the counter-notification procedures appear to serve the generally self-policing policy that section 512 reflects.”³²³⁰ Cybernet’s counter-notification procedures provided that, if an alleged infringer stated under penalty of perjury that it had removed the named infringing material, the alleged infringer’s access to the service would be restored. The court held that this policy “allows Cybernet to reinstate an infringer without the Congressionally-required statement and provides cover for Cybernet to water down its termination policy by treating these minimalist take-down statements as neither an admission

³²²⁷ Id. at 1178-79.

³²²⁸ Id. at 1179-80.

³²²⁹ Id. at 1180.

³²³⁰ Id.

nor a denial of the copyright infringement allegations, regardless of how blatant the infringement might be.”³²³¹

The court also concluded that the Section 512(c) safe harbor was not available for the further reason that Cybernet received a financial benefit “directly attributable” to infringing activity with respect to which it had the right and ability to control. The court noted that the direct financial benefit requirement was satisfied for the same reasons noted in its analysis of Cybernet’s vicarious liability (see Section II.C.3(d) above),³²³² although it agreed with the Hendrickson v. eBay and CoStar courts that the mere ability to exclude users from its system is not of itself sufficient right and ability to control infringing activity to deny the safe harbors to a service provider.³²³³ The court expressed no opinion on the question whether the “directly attributable” language in the safe harbor is narrower or equivalent to the general vicarious infringement requirement of a direct financial benefit, but ruled that in any event the direct flow of income to Cybernet based on the number of new subscribers signed up by its member sites at which infringing activity was taking place was sufficient to establish a financial benefit “directly attributable” to infringing activity.³²³⁴

Finally, the court held that there was no evidence presented that Cybernet ever “expeditiously” removed infringing material from its system, disabled links, or altered its search engine under its DMCA policy. Accordingly, the court concluded that there was little likelihood that Cybernet would qualify for the safe harbors.³²³⁵ (An additional aspect of the court’s ruling with respect to the Section 512(d) safe harbor is set forth in Section III.C.6(b)(1)(iv) below.)

Important Principles. The court’s interpretation of the obligations imposed on a service provider by Section 512(i) are interesting. Specifically, Section 512(i) is directed toward elimination of repeatedly infringing users, whereas Section 512(c) is directed to elimination of infringing materials. Thus, under “appropriate circumstances,” a service provider must deny all further service to a user who is repeatedly using the service to infringe, even if the service provider has in every instance removed the particular infringing material that has been identified. In the Perfect 10 v. Cybernet Ventures case, webmasters who had their sites taken down upon notice of infringing material would often simply set up a new site and continue offering infringing materials. The Perfect 10 v. Cybernet Ventures court ruled that in such circumstances, the defendant should have ceased allowing those webmasters to be a part of its service entirely, regardless of the site from which they were operating.

What constitutes an “appropriate circumstance” for denial of further services to a repeat infringer is unclear from the case. The court speaks of “blatant, repeat infringement by

³²³¹ Id.

³²³² Id. at 1181.

³²³³ Id.

³²³⁴ Id.

³²³⁵ Id. at 1182.

particular users, particularly infringement of a willful and commercial nature.”³²³⁶ This suggests a fairly high standard for an “appropriate circumstance.” However, the court also stated that these were circumstances in which a service provider should “at a minimum” terminate services to an infringer, so one cannot assume that blatant or willful infringements of a commercial nature are the only circumstances under which it would be “appropriate” to terminate a user.

The court’s rulings with respect to the notice requirements of Section 512(c) are also interesting. First, under those rulings, a service provider’s notification procedures must allow for notification of a representative list of copyright works being infringed, rather than always requiring an exact itemization of the allegedly infringed works. It is unclear from the opinion whether the representative list possibility must be an explicitly stated part of the service provider’s formal notification procedures, or whether it would be sufficient for the service provider to in fact accept such representative list and act on it. Second, the court interpreted the counter-notification procedures of the safe harbors in effect to require a statement by the alleged infringer that the allegedly infringing materials were in fact not infringing – i.e., that they were removed “as a result of mistake or misidentification of the material.”³²³⁷ It is not sufficient for the alleged infringer to inform the service provider that allegedly infringing materials have been removed. If the alleged infringer does not state that the materials were removed by mistake or misidentification, or at least somehow otherwise indicate that the materials were not infringing, the Perfect 10 v. Cybernet Ventures opinion suggests that the service provider is to treat the user as a knowing infringer with respect to that material and count a “strike” against the user for purposes of measuring whether the user is a “repeat infringer.”

e. The Aimster/Madster Lawsuits

The facts of the Aimster/Madster lawsuits are set forth in Section III.C.2(c)(3) above. In that case, Aimster asserted the Section 512(c) safe harbor. As discussed in Section III.C.6(b)(1)(i).c above, the district court concluded that Aimster was not entitled to any of the DMCA safe harbors because of its failure to satisfy the Section 512(i) predicate with respect to implementation of a policy to terminate repeat infringers on its system. In addition, the court held that Aimster had not satisfied the specific conditions of Section 512(c) because the plaintiffs were not asserting liability based on the caching of infringing material anywhere within Aimster’s system, and the infringing materials were not transmitted “through” the Aimster system.³²³⁸ As discussed in Section III.C.6(b)(1)(i).c, on appeal the Seventh Circuit affirmed the ruling that the safe harbors were not available to Aimster because of failure to comply with Section 512(i).³²³⁹

f. Hendrickson v. Amazon.com

³²³⁶ Id. at 1177.

³²³⁷ 17 U.S.C. § 512(g)(3)(C).

³²³⁸ In re Aimster Copyright Litigation, 252 F. Supp. 2d 634, 660-61 (N.D. Ill. 2002) & n.21.

³²³⁹ In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004).

The case of Hendrickson v. Amazon.com, Inc.³²⁴⁰ adjudicated the interesting issue of the extent of an ISP's obligation to police its system for infringing material once it receives notice from a copyright holder that all copies of a particular work are unauthorized. This case involved facts similar to the Hendrickson v. eBay case discussed above. On Jan. 28, 2002, Hendrickson sent a letter to Amazon.com notifying it that all copies of the movie *Manson* on DVD infringed his copyright. On Oct. 21, 2002, Hendrickson noticed that a *Manson* DVD was posted for sale on Amazon's website. Hendrickson purchased a copy of the DVD, then filed an action against both Amazon and the poster of the DVD, asserting claims of direct infringement against Amazon and the poster, and a claim of vicarious liability against Amazon. Amazon moved for summary judgment on the ground that it was not liable for direct infringement, since the movie had not been sold by Amazon, and that it was entitled to the safe harbor of Section 512(c) for the claim of vicarious liability.³²⁴¹

The court first ruled that Amazon was not liable for direct infringement, even though it had offered the website pages that the seller and buyer used to complete the purchase, because Amazon was not the actual seller of the item.³²⁴² With respect to the DMCA safe harbor, the court first held, consistent with the Aimster/Madster case and the Ninth Circuit's decision in Napster I, that the DMCA safe harbors can shield against vicarious liability.³²⁴³ The court then noted that, although the DMCA places the burden on the copyright owner in the first instance to monitor the Internet for potentially infringing sales,³²⁴⁴ "because the DMCA is relatively new, the question as to how long an adequate notice should remain viable is still unanswered."³²⁴⁵

Turning to an analysis of this question, the court noted that it was not the intention of Congress that a copyright owner could write one blanket notice to all service providers alerting them of infringing material, thereby relieving himself of any further responsibility and placing the onus forever on the service provider. However, the court also noted that it would be against the spirit of the DMCA if the entire responsibility were to lie with the copyright owner to forever police websites in search of possible infringers.³²⁴⁶

To resolve a balance between these competing concerns, the court looked to the language of the safe harbor, noting that to qualify for the safe harbor, Section 512(c) requires that the service provider not have actual knowledge that material on its system "is infringing" or that infringing activity "is apparent."³²⁴⁷ The court concluded that, by use of the present tense,

³²⁴⁰ 69 U.S.P.Q.2d 1471 (C.D. Cal. 2003).

³²⁴¹ Id. at 1471-72.

³²⁴² Id. at 1472.

³²⁴³ Id.

³²⁴⁴ Id. at 1473. In an earlier opinion, the court had ruled that Hendrickson's Jan. 2002 letter substantially complied with the DMCA notice requirements. Hendrickson v. Amazon.com, Inc., CV 02-07394 TJH (C.D. Cal. 2003).

³²⁴⁵ 69 U.S.P.Q.2d at 1473.

³²⁴⁶ Id.

³²⁴⁷ Id.

Congress intended for the notice to make the service provider aware of the infringing activity that is occurring at the time it receives the notice.³²⁴⁸ “If the infringing material *is on the website at the time* the ISP receives the notice, then the information, that all *Manson* DVD’s are infringing, can be adequate to find the infringing material expeditiously. However, if at the time the notice is received, the infringing material is not posted, the notice does not enable the service provider to locate infringing material that is not there, let alone do it expeditiously.”³²⁴⁹

Drawing on these principles, the court ruled that the DMCA places a limit on the viability of an otherwise adequate notice, and with respect to the instant case, “Hendrickson’s January, 2002, letter, claiming all *Manson* DVDs violate his copyright, although adequate for the listings then on Amazon, cannot be deemed adequate notice for subsequent listings and sales, especially, as here, when the infringing item was posted for sale nine months after the date of the notice.”³²⁵⁰ Accordingly, Amazon’s lack of knowledge of the infringing activity satisfied the first prong of the safe harbor under Section 512(c)(1)(A).³²⁵¹ Amazon satisfied the second prong of the safe harbor under Section 512(c)(1)(B) because, although it received a financial benefit from its third party sellers, the court held that there was no evidence to suggest that Amazon had “the ability to know that an infringing sale by a third party seller would occur,” and hence it could not control such sales.³²⁵² Accordingly, the court granted Amazon summary judgment under the safe harbor of Section 512(c).³²⁵³

g. Rossi v. MPAA

A peripheral issue relating to the notice provisions of the Section 512(c) safe harbor was raised in the case of Rossi v. Motion Picture Association of America, Inc.,³²⁵⁴ in which the plaintiff was the operator of a web site called internetmovies.com, an online directory of artists’ works and an Internet news magazine providing information and resources about movies on the Internet. The MPAA found statements on the web site such as “Join to download full length movies online now! New movies every month”; “Full Length Downloadable Movies”; and “NOW DOWNLOADABLE” followed by graphics from a number of the MPAA’s copyrighted movies. The MPAA sent a Section 512(c) written notice to the plaintiff’s Internet service provider asking that it remove the plaintiff’s web site from its server because of the site’s allegedly infringing content.³²⁵⁵

³²⁴⁸ Id.

³²⁴⁹ Id. at 1473-74 (emphasis in original).

³²⁵⁰ Id. at 1474.

³²⁵¹ Id.

³²⁵² Id.

³²⁵³ Id.

³²⁵⁴ Rossi v. Motion Picture Ass’n of America, Inc., 391 F.3d 1000 (9th Cir. 2004).

³²⁵⁵ Id. at 1002.

The plaintiff sued the MPAA for, among other things, tortious interference with contractual relations and tortious interference with prospective business advantage, and the MPAA moved for summary judgment. Under Hawaiian law, the plaintiff was required to show that the MPAA acted without justification. The MPAA argued that its actions were justified because the DMCA authorized it to send the plaintiff's Internet service provider a notice requesting that it shut down the plaintiff's web site.³²⁵⁶

The plaintiff argued that the MPAA was not justified in sending the DMCA notice because, in order to have "a good faith belief" of infringement, the copyright owner is required to conduct a reasonable investigation into the allegedly offending website. The plaintiff argued that the reasonableness of the investigation should be judged under an objective standard of review, and that the MPAA had failed to meet that standard because, if it had reasonably investigated the site by attempting to download movies, it would have discovered that no movies could actually be downloaded from the site or related links.³²⁵⁷

The MPAA countered that the "good faith belief" requirement should be a subjective one, and the Ninth Circuit agreed. Although no court had yet interpreted the standard under Section 512(c), the court noted that several decisions interpreting other federal statutes had traditionally interpreted "good faith" to encompass a subjective standard. The court also found that the overall structure of Section 512 supported the conclusion that Section 512(c)(2)(A)(v) imposes a subjective good faith requirement on copyright owners. Congress included in Section 512(f) a limited cause of action for improper infringement notifications, imposing liability only if the copyright owner's notification is a knowing misrepresentation. Juxtaposing the "good faith" proviso of the DMCA with the "knowing misrepresentation" provision revealed a statutory structure intended to protect potential violators only from subjectively improper actions by copyright owners.³²⁵⁸

The Ninth Circuit found that the plaintiff had failed to raise a genuine issue of material fact under the subjective standard regarding the MPAA's good faith. The statements on the plaintiff's web site strongly suggested that movies were available for downloading, and the court noted that the plaintiff had admitted that his own customers often believed that movies were available for downloading. Accordingly, the Ninth Circuit affirmed the district court's ruling on summary judgment that there was no issue of material fact as to the MPAA's "good faith belief" that the plaintiff's web site was infringing its copyrights.³²⁵⁹ The Ninth Circuit also affirmed the district court's holding that the MPAA's good faith compliance with the notice and takedown

³²⁵⁶ Id.

³²⁵⁷ Id. at 1003-04.

³²⁵⁸ Id. at 1004-05.

³²⁵⁹ Id. at 1005-06.

procedures of the DMCA constituted sufficient “justification” under Hawaiian law to avoid the plaintiff’s claim for tortuous interference with contractual relations.³²⁶⁰

h. Perfect 10 v. CCBill

The facts of this case are set forth in Section III.C.6(b)(1)(i)d. above. In that case, the defendant CWIE, an OSP hosting various sites that allegedly contained infringing copies of Perfect10’s photos, moved for summary judgment under the Section 512(c) safe harbor. Perfect 10 argued that CWIE was not entitled to the safe harbor because it had actual knowledge of Perfect 10’s infringements on its clients’ web sites, it was aware of facts or circumstances from which infringing activity was apparent, it failed to expeditiously remove or disable access to infringing material of which it had knowledge, and it received a financial benefit directly attributable to the infringing activity and had the right and ability to control such activity.³²⁶¹

With respect to the issue of knowledge, the district court found Perfect 10’s notifications to CWIE of infringement to be deficient under Section 512(c) because they identified only the web sites containing allegedly infringing material, but did not identify the URLs of the infringing images or which of Perfect 10’s copyrights were being infringed.³²⁶² With respect to whether CWIE had constructive notice of infringement, the court noted that the kind of constructive notice Congress contemplated under Section 512(c) was that of “red flag” web sites from which infringements would be apparent based on a cursory review of the web site. Under this test, although some of CWIE’s affiliate web sites advertised images of celebrities, they did not contain obvious infringements because the web sites did not advertise themselves as pirate web sites. Accordingly, the court concluded that Perfect 10 had not raised a genuine issue of material fact that CWIE had actual or constructive knowledge of infringements on its clients’ web sites.³²⁶³

With respect to the issue of control, the court noted that CWIE’s right and ability to control infringing activity was limited to disconnecting its webmasters’ access to CWIE’s service. Citing the case of Perfect 10 v. Cybernet Ventures, Inc.,³²⁶⁴ the court ruled that the mere ability to terminate services to a web site was not sufficient control for purposes of the Section 512(c) safe harbor. Nor was the fact that CWIE reviewed its sites to look for blatantly illegal and criminal conduct sufficient to close the safe harbor, for the DMCA was intended to encourage OSPs to work with copyright owners to locate and stop infringing conduct. Accordingly, the court ruled that CWIE was entitled to summary judgment on the Section 512(c) safe harbor.³²⁶⁵

³²⁶⁰ Id. at 1006.

³²⁶¹ Perfect 10, Inc. v. CCBill, 340 F. Supp. 2d 1077, 1103 (C.D. Cal. 2004).

³²⁶² Id. at 1100-01.

³²⁶³ Id. at 1103-04.

³²⁶⁴ 213 F. Supp. 1146, 1181 (C.D. Cal. 2002).

³²⁶⁵ Perfect 10, Inc. v. CCBill, 340 F. Supp. 2d at 1104-05.

On appeal, the Ninth Circuit, for the reasons discussed above in Section III.C.6(b)(1)(i).d above, agreed with the district court's rulings that Perfect 10's notices of infringement were insufficient to comply with the requirements of Section 512(c)(3) or to provide CWIE with knowledge or awareness within the standard of Section 512(c)(1)(A).³²⁶⁶ The remaining question was therefore whether Perfect 10 had raised a genuine issue of material fact concerning whether CWIE received a direct financial benefit from the infringing activity.³²⁶⁷ The Ninth Circuit held that "'direct financial benefit' should be interpreted consistent with the similarly-worded common law standard for vicarious liability. ... Thus, the relevant inquiry is 'whether the infringing activity constitutes a draw for subscribers, not just an added benefit.'"³²⁶⁸ The court noted that Perfect 10 had alleged only that CWIE hosted websites for a fee, and such allegation was insufficient to show that the infringing activity was a draw. The court also noted that legislative history of Section 512 stated that receiving a one-time set-up fee and flat, periodic payments for service from a person engaging in infringing activities would not constitute receiving a direct financial benefit. Accordingly, the court ruled that there was no genuine issue that CWIE had received a direct financial benefit from infringing activity, and therefore if on remand the district court were to find that CWIE had met the threshold requirements of Section 512(i), CWIE would be entitled to the Section 512(c) safe harbor.³²⁶⁹

i. Corbis Corp. v. Amazon.com, Inc.

The opinion in this case contains a lengthy adjudication of the requirements of Section 512(i) as a predicate for the Section 512 safe harbors. Amazon hosted through its website a platform called "zShops," which allowed individuals and retailer vendors to showcase their products and sell them directly to online consumers. A zShop vendor could include a product image in its sales listing in one of two ways – either by creating a link to an image stored on the vendor's computer or server, or by uploading an image to one of Amazon's servers for display in the listing. Amazon did not actively participate or supervise the uploading or linking of images, nor did it preview the images before the link was created or the upload completed.³²⁷⁰

Corbis, the owner of the copyrights in a large collection of images, brought copyright claims against Amazon because 230 of its images were displayed and sold without authorization by zShop vendors through the Amazon website. In addition, two other images were displayed by Amazon in banner ads that appeared on the Internet Movie Database (IMDb), a website owned by Amazon and operated separately from Amazon.com. Amazon asserted the safe harbor of Section 512(c).³²⁷¹

³²⁶⁶ Perfect 10, Inc. v. CCBill, 481 F.3d 751, 766 (9th Cir.), cert. denied, 552 U.S. 1062 (2007).

³²⁶⁷ Id.

³²⁶⁸ Id. at 767 (quoting Ellison v. Robertson, 357 F.3d 1072, 1078-79 (9th Cir. 2004)).

³²⁶⁹ 481 F.3d at 767.

³²⁷⁰ Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1094 (W.D. Wa. 2004).

³²⁷¹ Id. at 1096-98.

The court turned first to a very detailed analysis of whether Amazon satisfied all the predicate conditions of Section 512(i):

– Whether Amazon was a “Service Provider”. The court ruled that Amazon clearly qualified under the definition of “Service Provider” of Section 512(k)(1)(B), and rejected Corbis’ argument that a Service Provider must “serve to route or connect online digital communications.” Amazon’s operation of web sites was sufficient to make it a Service Provider.³²⁷²

– Whether Amazon Had Adopted an Adequate User Policy. Amazon required all zShop vendors to execute a Participation Agreement, which prohibited vendors from listing or linking to any item that infringed any third party intellectual property right or was counterfeited, illegal, stolen, or fraudulent. The agreement also gave Amazon the right, but not the obligation, to monitor any activity and content associated with the site, and the right and the absolute discretion to remove, screen, or edit any content that violated the agreement or was otherwise objectionable.³²⁷³ In addition, it was Amazon’s policy that when it received information that a vendor might be infringing another’s copyrights, it would cancel the allegedly infringing listing and send an email to the vendor, notifying it of the cancellation, identifying a contact email address for the complaining party, and reminding the vendor that “repeated violations of our Community Rules could result in permanent suspension from our Auction, zShops, and Amazon Marketplace sites.”³²⁷⁴

Corbis complained that the Participation Agreement and Amazon’s related policies were too vague with respect to copyright infringement, in that they did not include the term “repeat infringer” and did not describe the methodology employed in determining which users would be terminated for repeated copyright violations. The court rejected this argument, noting that the language of Section 512(i) and the overall structure of the DMCA indicate that the user policy need not be as specific as Corbis suggested. The fact that Congress left the phrase “repeat infringer” undefined, and chose not to elaborate on what circumstances merit terminating a repeat infringer’s access, suggested Congress’ intent to leave the policy requirements and the obligations of service providers loosely defined.³²⁷⁵ “Given the complexities inherent in identifying and defining online copyright infringement, § 512(i) does not require a service provider to decide, *ex ante*, the specific types of conduct that will merit restricting access to its services. As Congress made clear, the DMCA was drafted with the understanding that service providers need not ‘make difficult judgments as to whether conduct is or is not infringing.’”³²⁷⁶

³²⁷² *Id.* at 1100 & n. 6.

³²⁷³ *Id.* at 1095.

³²⁷⁴ *Id.*

³²⁷⁵ *Id.* at 1100-01.

³²⁷⁶ *Id.* at 1101.

The court found that the Participation Agreement adequately prohibited the listing, linking, or posting of any material that violates copyright laws and made clear that those who violated Amazon’s policies could face a variety of penalties. In addition, the court pointed to testimony that those accused of copyright infringement were informed that repeated violations could result in “permanent suspension” from Amazon sites. Accordingly, the court ruled that Amazon had an adequate user policy.³²⁷⁷

– Whether Amazon Had Adequately Communicated Its Termination Policy to Its Users. Corbis argued that Amazon had not adequately communicated its termination policy to its users because it did not inform them of the internal criteria it used to determine whether to terminate a user’s access to the site. The court held, however, that Section 512(i) is not so exacting, and that Amazon needed only inform users that, in appropriate circumstances, it may terminate the user’s accounts for repeated copyright infringement. The statute does not suggest what criteria should be considered by a service provider, much less require the service provider to reveal its decision making criteria to the user. Amazon was required only to put users on notice that they faced exclusion from the service if they repeatedly violate copyright law, and Amazon had done so.³²⁷⁸

– Whether Amazon Had Reasonably Implemented Its Infringement Policy. To judge the adequacy of implementation of an infringement policy, the court noted that one must look at two questions – whether a service provider has adopted a procedure for receiving complaints and conveying those complaints to users, and whether the service provider nonetheless still tolerates flagrant or blatant copyright infringement by its users.³²⁷⁹

Turning to the first question, the court found that Amazon had a sufficient procedure for implementing its infringement policy. Amazon had a practice to promptly cancel a listing once it received adequate notice that the listing violated another’s copyrights, to inform the vendor that its listing may have violated intellectual property rights, to give the vendor the contact information of the complaining party, and to warn the vendor that repeated violations could result in permanent suspension from the Amazon site. The fact that certain vendors had been able to reappear on the zShops platform under pseudonyms did not amount to a failure of implementation. The court ruled that an infringement policy need not be perfect; it need only be reasonably implemented. Corbis had not shown any more effective and reasonable method that Amazon could have used to prevent vendors from re-accessing zShops.³²⁸⁰

With respect to the second question – tolerance of flagrant abusers – the court noted that Section 512(i) requires only that repeated copyright infringers be terminated in “appropriate circumstances” and that a service provider need not conduct active investigation of

³²⁷⁷ Id.

³²⁷⁸ Id. at 1101-02.

³²⁷⁹ Id. at 1102.

³²⁸⁰ Id. at 1103-04.

possible infringement or make a decision regarding difficult infringement issues.³²⁸¹ The court seems to have set a rather high threshold for what might constitute “appropriate circumstances”: “Because it does not have an affirmative duty to police its users, failure to properly implement an infringement policy requires a showing of instances where a service provider fails to terminate a user even though it has sufficient evidence to create actual knowledge of that user’s blatant, repeated infringement of a willful and commercial nature.”³²⁸²

Corbis alleged that Amazon tolerated repeated infringers because it had received three emails (although not from Corbis) in which the sender claimed that zShop listings posted by one vendor were infringing, and had received seven emails (again not from Corbis) in which the sender claimed that zShop listings of another vendor were infringing, and had not terminated either vendor’s access to zShops until after Corbis’ suit was filed. The court found that this evidence did not amount to a showing that Amazon had knowledge of blatant, repeat infringement that would have required Amazon to terminate access to the vendors’ zShops sites.³²⁸³ In a very significant ruling, the court held the following: “Although efforts to pin down exactly what amounts to knowledge of blatant copyright infringement may be difficult, it requires, at a minimum, that a service provider who receives notice of a copyright violation be able to tell merely from looking at the user’s activities, statements, or conduct that copyright infringement is occurring.”³²⁸⁴ Citing various previously decided cases, the court noted that examples of such blatant infringement may include statements from the vendor that a product is bootlegged or pirated, chat rooms hosted by the service provider in which users discuss how the service can be used to circumvent copyright laws, or the offering of hundreds of audio files in a single day for peer to peer copying. Corbis had presented no such examples of blatant infringing activity on the vendor defendants’ zShops sites.³²⁸⁵

In another significant ruling, the court held that notices from copyright owners under Section 512(c)(3) do not, of themselves, necessarily establish evidence of blatant or repeat infringement. “A copyright owner may have a good faith belief that her work is being infringed, but may still be wrong. The notification requirement does not take into account that a vendor may have ‘a legitimate fair use defense, or can otherwise invoke any of the myriad other factors that go into evaluating a copyright infringement claim.’ Although the notices have brought the listings to Amazon’s attention, they did not, in themselves, provide evidence of blatant copyright infringement.”³²⁸⁶ The court ruled that knowledge of blatant, repeat infringement cannot be imputed merely from the receipt of notices of infringement. Instead, there must be additional evidence available to the service provider to buttress the claim of infringement supplied by the

³²⁸¹ Id. at 1104.

³²⁸² Id.

³²⁸³ Id. at 1104.

³²⁸⁴ Id. at 1104-05.

³²⁸⁵ Id. at 1005.

³²⁸⁶ Id. (citation omitted).

notices.³²⁸⁷ The court went on to state, “In this regard, this Court respectfully disagrees with CCBill, in which the district court for the Central District of California held that receipt by the service provider of two or more DMCA compliant notices about one of its users required termination under § 512(i). Although there may be instances in which two or more DMCA compliant notices make a service provider aware of a user’s blatant, repeat infringement, the notices alone do not make the user’s activity blatant, or even conclusively determine that the user is an infringer.”³²⁸⁸

The court noted that, other than the Section 512(c)(3) email notices of infringement, there was no evidence suggesting that Amazon would have been able to tell, merely by looking at the listings of the two vendors, that the posters and photos being sold infringed another’s copyrights. Without some evidence from the site raising a red flag, Amazon would not know enough about the photograph, the copyright owner, or the user to make a determination that the vendor was engaging in blatant copyright infringement. In addition, one of the vendors had unequivocally stated to Amazon that it had the right to sell all of the posters in its inventory. The other vendor had told Amazon that all of its products were officially licensed. The court concluded that for Amazon to determine that the two vendors were infringers, it would have had to conduct the type of investigation that the courts and Congress had found unnecessary.³²⁸⁹

– Whether Amazon Had Knowledge of Infringement. Having concluded that Amazon satisfied all predicate conditions of Section 512(i), the court then turned to the conditions of the Section 512(c) safe harbor that Amazon had to establish – that it did not have knowledge of infringing activity or acted expeditiously to remove infringing materials upon gaining knowledge, and that it did not receive a financial benefit directly attributable to any infringing activity that it maintained the right and ability to control. Because Corbis did not challenge Amazon’s claim that it acted expeditiously to remove or disable access to allegedly infringing material, the court turned to the knowledge and control prongs.³²⁹⁰

In view of the fact that Corbis did not challenge that Amazon expeditiously removed access to allegedly infringing material, it is somewhat curious that the court engaged in such an extensive analysis of the knowledge prong of the Section 512(c) safe harbor. Nevertheless, the court issued some important rulings about the knowledge prong that were consistent with its other rulings to afford a broad scope to the Section 512(c) safe harbor.

Because Corbis had chosen not to send notices of infringement to Amazon before filing its lawsuit, Amazon had no actual knowledge of the alleged infringements of Corbis’ copyrighted images, and the court turned its analysis to whether Corbis was aware of facts or circumstances

³²⁸⁷ Id. at 1105-06.

³²⁸⁸ Id. at 1105 n.9 (citation omitted).

³²⁸⁹ Id. at 1106.

³²⁹⁰ Id. at 1106-07.

from which infringing activity was apparent. Corbis submitted evidence of notices provided by other copyright holders addressing non-Corbis photos and evidence suggesting that Amazon was aware that Corbis licensed celebrity photos, from which Corbis argued that Amazon should have known that zShops vendors sold infringing Corbis images.

The court rejected this evidence as insufficient to establish a material issue of fact regarding Amazon's actual or apparent knowledge of infringing material on the zShops platform. A mere general awareness that a particular type of item may be easily infringed is insufficient to establish actual knowledge. With respect to apparent knowledge, the court cited the Nimmer copyright treatise for the proposition that the standard is not "what a reasonable person would have deduced given all the circumstances," but rather "whether the service provider deliberately proceeded in the face of blatant factors of which it was aware."³²⁹¹ The court also quoted from the legislative history of the DMCA that apparent knowledge requires evidence that a service provider "turned a blind eye to 'red flags' of obvious infringement."³²⁹²

To establish apparent knowledge, Corbis submitted evidence that Amazon received notices that zShops vendors were infringing the copyrights of unrelated parties by selling celebrity photographs. The court found this evidence insufficient, because it was not clear whether any of the vendors receiving such notices were vendors in the instant litigation and whether the notices complied with the requirements of Section 512(c)(3). If the notices were compliant, Amazon asserted that it promptly canceled a listing after receiving a notice of infringement, an assertion that Corbis did not challenge.³²⁹³

In any event, in a more significant ruling, the court held that third party notices do not, in themselves, constitute red flags. As noted in the legislative history, evidence of blatant copyright infringement will often derive from information on the offending site itself. The court noted that even if the notices had caused Amazon to examine the content of the zShops sites, Corbis had not shown that those sites contained the type of blatant infringing activity that would have raised a red flag for Amazon. Accordingly, Corbis had failed to establish apparent knowledge of infringement on the part of Amazon.³²⁹⁴

– Whether Amazon Had the Right and Ability to Control the Infringing Activity. Corbis argued a right and ability to control on Amazon's part from the fact that it had terminated the zShops defendants on the same day Corbis filed and served its complaint. The court cited the CCBill and Costar cases for the proposition that the right and ability to control prong cannot be satisfied merely by the ability of a service provider to remove or block access to materials posted on its website or stored on its systems. Nor did the fact that Amazon advertised the zShops platform amount to a right and ability to control the items sold there absent some showing that

³²⁹¹ *Id.* at 1108 (quoting 3 M. Nimmer & D. Nimmer, *Nimmer on Copyright* § 12B.04[A][1], at 12B-49 (2004)).

³²⁹² *Corbis*, 351 F. Supp. 2d at 1108 (citing H.R. Rep. No. 105-551 Part 2, at 42 (1998)).

³²⁹³ *Corbis*, 351 F. Supp. 2d at 1108.

³²⁹⁴ *Id.* at 1108-09.

Amazon intended to pick infringing material for its site. The court noted that Amazon did not preview the products prior to their listing, did not edit the product descriptions, and did not suggest prices or otherwise involve itself in the sale. Accordingly, the court ruled that Amazon did not have the right and ability to control the infringing material, and the court therefore did not need to look into whether Amazon received a direct financial benefit from the allegedly infringing conduct.³²⁹⁵

Based on its various rulings, the court concluded that Amazon was entitled to the Section 512(c) safe harbor and was therefore immune from all monetary relief. The only relief Corbis could be entitled to was the limited injunctive relief set forth in Section 512(j). Because Corbis had not sought injunctive relief, and because Amazon had asserted that it had terminated the accounts of the defendant vendors, it was unclear how the limited injunctive relief would apply in the particular case at bar. The court therefore granted Amazon's motion for summary judgment with respect to the DMCA claims.³²⁹⁶

j. **Tur v. YouTube, Inc.**

In Tur v. YouTube, Inc.,³²⁹⁷ Robert Tur, owner of the copyright in video footage of the Reginald Denny beatings during the 1992 Los Angeles riots, sued YouTube for copyright infringement based on the unauthorized presence of his copyrighted video footage on the web site. YouTube moved for summary judgment under the Section 512(c) safe harbor. The court denied summary judgment, finding that there were factual issues with respect to whether YouTube had the right and ability to control infringing activity on its site. The court agreed with existing precedents that the right and ability to control requires more than just the ability of a service provider to remove or block access to materials posted on its web site or stored on its system.³²⁹⁸ "Rather, the requirement presupposes some antecedent ability to limit or filter copyrighted material."³²⁹⁹ The court found, however, that there was insufficient evidence in the record regarding the process undertaken by YouTube from the time a user submitted a video clip to the point of display on the YouTube site, and the extent of YouTube's technical capabilities to detect and pre-screen allegedly infringing videos.³³⁰⁰ On Oct. 19, 2007, the court granted Tur's motion to voluntarily dismiss his complaint so that he could join as a plaintiff in class action litigation filed by The Football Association Premier League Limited against YouTube on May 4, 2007 in the Southern District of New York.³³⁰¹

³²⁹⁵ Id. at 1109-10.

³²⁹⁶ Id. at 1110-11 & 1118-19.

³²⁹⁷ 2007 U.S. Dist. LEXIS 50254 (C.D. Cal. June 20, 2007).

³²⁹⁸ Id. at *9.

³²⁹⁹ Id.

³³⁰⁰ Id. at *10.

³³⁰¹ Order Granting Plaintiff's Motion to Voluntarily Dismiss Complaint, Tur v. YouTube, Inc., CV 06-4436 FMC (C.D. Cal. Oct. 19, 2007).

k. Io Group v. Veoh Networks

In Io Group, Inc. v. Veoh Networks, Inc.,³³⁰² a decision by a magistrate judge, Veoh operated a user-generated content web site through which users could also access videos from Veoh's content partners. Once video files were uploaded to Veoh's system, Veoh's employees selected videos to be featured on the "Featured Videos" portion of the web site. A number of clips submitted by users contained content from the Io Group's copyrighted sexually explicit videos, and Io Group sued Veoh for copyright infringement for hosting the clips, without giving prior notice to Veoh or demanding that Veoh take down the allegedly infringing material. Veoh asserted the safe harbor under Section 512(c).³³⁰³

Before users could upload videos to Veoh's site, they were required to register and agree to abide by the Terms of Use and Acceptable Use policies posted on the site. The Terms of Use stated that Veoh reserved the right to monitor user-submitted material and to remove it from the site, that the user was not permitted to publish or make available any material that infringed third party intellectual property rights, and that the user represented and warranted that it had all rights necessary to publish and distribute any material submitted to the site. Upon each upload of particular material, the user was presented with an explicit reminder that it must not upload copyrighted, pornographic, obscene, violent, or other videos that violate Veoh's applicable policies. Upon receiving a notice that a user had uploaded infringing content after a first warning, the user's account would be terminated, all content provided by that user disabled (unless the content was also published by another non-terminated user and was not the subject of a DMCA notice), and the user's email address would be blocked so that a new account could not be opened with that same address. Veoh also had the ability to disable access to such material on its users' hard drives if their computers were still connected to the Internet, and it had adopted means for generating a digital fingerprint for each video file that enabled Veoh to terminate access to any other identical files and prevent additional identical files from ever being uploaded by any user.³³⁰⁴

When users uploaded a video to Veoh's system, they would provide certain metadata about the video, including title, description, tags, selection of up to four categories best describing the video, and a content rating. Upon receiving a video submission, Veoh's computers would first confirm that the submitted file was, in fact, a video file with a compatible codec, and if so, the system would extract the file format and length, assign a unique video ID number to it, index the user-entered metadata and store the information in a database on Veoh's servers. The database also automatically indexed video files into a series of lists, such as "Most Recent," "Top Rated," "Most Popular," "Most Discussed," and "Top Favorite." In addition to saving the file in its original format, which users could download using Veoh's client software, the system also automatically converted the file into Flash format. The system also extracted during the upload process 16 full resolution screen captures (screencaps) and 16 lower

³³⁰² 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

³³⁰³ Id. at 1135-36.

³³⁰⁴ Id. at 1137-38.

resolution screenshots. One of the lower resolution screenshots was used to represent the video in a search result which, when clicked on, took the user to a video details page containing the video and a link to view all 16 lower resolution screenshots. Veoh employees occasionally spot checked videos after publication for compliance with Veoh's policies and to ensure accuracy in the description and characterization of the content, and on occasion edited the video description field. If a spot check revealed an instance of blatant copyright infringement (e.g., a movie known to have been released only in theaters), Veoh disabled access to the material.³³⁰⁵

The court rejected Io Group's argument that Veoh had not implemented its repeat infringer policy in a reasonable manner. The court found that Veoh's evidence established that it had a working notification system and a procedure for dealing with copyright infringement notices. Veoh's policies identified its designated copyright agent and it often responded to infringement notices the same day received, or at most within a few days. When Veoh received notice that a user had uploaded infringing content after a first warning, the user's account was terminated and all content provided by that user was disabled. Veoh's fingerprint technology enabled it to terminate access to any other identical files and prevent additional identical files from ever being uploaded by any user. Since the web site was launched, Veoh had terminated 1,096 users for repeat copyright violations.³³⁰⁶

Io Group argued that Veoh's policy failed because it did not prevent repeat infringers from reappearing on the site under a pseudonym and a different email address. The court rejected this argument, ruling that the hypothetical possibility that a rogue user might reappear under a different user name and identity did not raise a genuine fact issue as to the implementation of Veoh's policy. Io Group had presented no evidence that a repeat infringer had, in fact, established a new account under false pretenses, much less that Veoh had intentionally allowed that to happen. The court rejected Io Group's reliance on the Napster case as establishing a requirement under Section 512(i) that a site operator track users by their actual names or IP addresses. Io Group had presented no evidence suggesting that tracking or verifying users' actual identity or that blocking their IP addresses would be a more effective reasonable means of implementation, particularly given that IP addresses identify only a particular computer connected to the Internet and not particular users. The court ruled that Section 512(i) does not require service providers to track users in a particular way or to affirmatively police users for evidence of repeat infringement. Veoh's tracking of content that had been identified as infringing and permanently blocking that content from ever being uploaded by any user was adequate to satisfy Section 512(i) requirements.³³⁰⁷

The court then turned to whether the requirements of the Section 512(c) safe harbor had been satisfied. Io Group argued that the Flash files and screenshots created during the publication process were not stored on Veoh's system "at the direction of a user," but by Veoh's own acts and decisions, and that Section 512(c) was not intended to protect the creation of

³³⁰⁵ Id. at 1138-40.

³³⁰⁶ Id. at 1143.

³³⁰⁷ Id. at 1143-45.

those files because Veoh used them as a means of distribution (e.g., by indexing content and organizing them into lists), and not just storage. The court rejected this argument, noting that the broader definition of “service provider” under Section 512(k)(1)(B) does not contain an express limitation that the content of material stored on the system not be modified. And existing case law such as the CoStar v. LoopNet decision supported the conclusion that Veoh was not precluded from the Section 512(c) safe harbor by virtue of its automated processing of user-submitted content. The court noted that Veoh did not itself actively participate or supervise the uploading of files, nor did it preview or select the files before the upload was completed. Instead, video files were uploaded through an automated process that was initiated entirely at the volition of Veoh’s users. Inasmuch as the conversion to Flash format was a means of facilitating user access to material on its web site, the court held that Veoh did not lose the safe harbor through the automated creation of those files.³³⁰⁸

Turning to the issue of knowledge of the infringing activity, the court found that, because Io Group had provided Veoh no notice of any claimed copyright infringement before filing its lawsuit, Veoh had no actual knowledge of the infringing activity at issue. With respect to knowledge through signs of apparent infringing activity, the court noted the applicable “red flag” test, which requires the service provider to be aware of blatant factors indicating infringement. The court found no such factors present in the instant case. None of the allegedly infringing video files uploaded by Veoh’s users contain Io Group’s copyright notices. Although one of the works did contain the plaintiff’s trademark several minutes into the clip, there was no evidence from which it could be inferred that Veoh was aware of, but chose to ignore, it. Nor would the professionally created nature of submitted content constitute a red flag per se, particularly given that the video equipment available to the general public was of such quality that there might be little distinction left between professional and amateur productions. Finally, the court rejected Io Group’s argument that Veoh should have known that no legitimate producer of sexually explicit material would have omitted the labels required by federal law for sexually explicit material identifying where records as to the performers depicted are kept. The court ruled that the absence of such labels did not give rise to a genuine issue of material fact as to whether Veoh had the requisite level of knowledge or awareness that the plaintiff’s copyrights were being violated.³³⁰⁹

With respect to the requirement to act expeditiously to remove or disable access to material, undisputed evidence established that when Veoh received DMCA-compliant notices, it responded and removed noticed content on the same day the notice was received or within a few days thereafter. In addition, Veoh also promptly investigated other complaints about content on its web site through a “Flag It!” feature that enabled users to bring certain content to Veoh’s attention by flagging it from a set list of reasons such as mis-rated content, sexually explicit content, and obscene content. Io Group argued that Veoh had willfully blinded itself to facts suggesting infringement because the list of reasons on the “Flag It!” feature no longer contained a choice for “appears to contain copyrighted material.” The court rejected this

³³⁰⁸ Id. at 1146-48.

³³⁰⁹ Id. at 1148-49.

argument, noting that the “Flag It!” feature itself contained a notice, prominently displayed at the top of the “Flag It!” dialog box, directing copyright owners to a link with instructions for submitting a copyright infringement notice to Veoh.³³¹⁰

Finally, with respect to the issue of right and ability to control the infringing activity, the court rejected Io Group’s argument that the requisite “right and ability to control” was present because Veoh had established and enforced policies prohibiting users from engaging in a host of illegal and other conduct on its web site and exercised the right to police its system by conducting occasional spot checks of video files for compliance. The court noted that the plaintiff was focused on the wrong inquiry. Under Section 512(c), the pertinent inquiry was not whether Veoh had the right and ability to control its *system*, but rather whether it had the right and ability to control the *infringing activity*. The latter cannot simply mean the ability of a service provider to block or remove access to materials posted on its web site. The court distinguished the Napster system, which existed solely to provide the site and facilities for copyright infringement, and Napster’s control over its system was directly intertwined with its ability to control infringing activity. In the instant case, by contrast, Veoh’s right and ability to control its system did not equate to the right and ability to control infringing activity. Unlike Napster, there was no suggestion that Veoh aimed to encourage copyright infringement on its system or that it could control what content users chose to upload before it was uploaded. Given that Veoh received hundreds of thousands of video files from its users, the court ruled that no reasonable juror could conclude that a comprehensive review of every file would be feasible. And even if it were, there could be no assurance that Veoh could have accurately identified the infringing content at issue. Accordingly, Veoh’s ability to control its index did not equate to an ability to identify and terminate *infringing* videos. For the most part, the files in question did not bear titles resembling the plaintiff’s works and the plaintiff had not provided Veoh with its titles to search.³³¹¹

The court further observed that, perhaps most importantly, there was no indication that Veoh had failed to police its system to the fullest extent permitted by its architecture. Once content had been identified as infringing, Veoh’s digital fingerprint technology prevented the same infringing content from ever being uploaded again, indicating that Veoh had taken steps to reduce, not foster, the incidence of copyright infringement on its web site. The court rejected Io Group’s argument that Veoh should have verified the source of all incoming videos by obtaining and confirming the names and addresses of the submitting user, the producer, and the submitting user’s authority to upload a given file, as required by California Penal Code § 653w and 18 U.S.C. § 2257. The court noted that the issue was not Veoh’s compliance with those statutory requirements, nor whether it should have been aware that certain content was infringing. Rather, the question was whether Veoh declined to exercise a right to stop it.³³¹² “Declining to change business operations is not the same as declining to exercise a right and

³³¹⁰ Id. at 1149-50.

³³¹¹ Id. at 1150-53.

³³¹² Id. at 1153-54.

ability to control infringing activity.”³³¹³ The plaintiff’s suggestion that Veoh must be required to reduce or limit its business operations was contrary to one of the stated goals of the DMCA to facilitate the growth of electronic commerce.³³¹⁴

Accordingly, the court granted Veoh’s motion for summary judgment under the Section 512(c) safe harbor. It cautioned however, that

the decision rendered here is confined to the particular combination of facts in this case and is not intended to push the bounds of the safe harbor so wide that less than scrupulous service providers may claim its protection. Nevertheless, the court does not find that the DMCA was intended to have Veoh shoulder the entire burden of policing third-party copyrights on its website (at the cost of losing its business if it cannot). Rather, the issue is whether Veoh takes appropriate steps to deal with copyright infringement that takes place. The record presented demonstrates that, far from encouraging copyright infringement, Veoh has a strong DMCA policy, takes active steps to limit incidents of infringement on its website and works diligently to keep unauthorized works off its website.³³¹⁵

I. UMG Recordings v. Veoh Networks (aff’d sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC)

The District Court Decisions

The case of UMG Recordings, Inc. v. Veoh Networks, Inc.³³¹⁶ involved the same user-generated content site, Veoh Networks, as the case described in the previous subsection. The plaintiffs, who owned rights to copyrighted sound recordings and musical compositions allegedly used without authorization in user-submitted videos to the site, sought summary judgment that Veoh was not entitled to the Section 512(c) safe harbor because of four functions performed by Veoh’s software that the plaintiffs claimed were not “storage” and were not undertaken “at the direction of the user”: automatically creating Flash formatted copies of video files uploaded by users, automatically creating copies of uploaded video files that are comprised of smaller chunks of the original file, allowing users to access uploaded videos via streaming, and allowing users to access uploaded videos by downloading whole video files. The court denied the plaintiff’s motion.³³¹⁷

The court noted that the IoGroup case had held that Section 512(c) was applicable to the creation of Flash formatted files, but the applicability of Section 512(c) to the other three

³³¹³ Id. at 1154.

³³¹⁴ Id.

³³¹⁵ Id. at 1155.

³³¹⁶ 620 F. Supp. 2d 1081 (C.D. Cal. 2008), aff’d sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013).

³³¹⁷ Id. at 1083.

challenged software functions was a question of first impression.³³¹⁸ Although the plaintiffs conceded that all four challenged software functions were directed toward facilitating access to materials stored at the direction of users, they argued that Section 512(c) requires that the service provider's conduct *be* storage, and that the storage be at the direction of a user. The court rejected this argument, finding that the safe harbor extends to functions other than mere storage, since the statutory language applies to "infringement of copyright *by reason of* the storage at the direction of a user."³³¹⁹ When copyrighted content was displayed or distributed on Veoh's system it was by reason of or attributable to the fact that users uploaded the content to Veoh's servers to be accessed by other means.³³²⁰ The court therefore denied the plaintiffs' motion for summary judgment, concluding:

The four software functions that UMG challenges fall within the scope of § 512(c), because all of them are narrowly directed toward providing access to material stored at the direction of users. Both the conversion of uploaded files into Flash format and the "chunking" of uploaded files are undertaken to make it easier for users to view and download movies, and affect only the form and not the content of the movies; "streaming" and downloading merely are two technically different means of accessing uploaded videos.³³²¹

Following this ruling, Veoh moved for summary judgment that it had satisfied the remaining requirements of Section 512(c) and was therefore not liable for monetary or injunctive relief. The court granted Veoh's motion for summary judgment.³³²² Because the basic facts of the case were not disputed, the court's opinion addressed the significant question of the extent to which the DMCA obligates Internet-based services like Veoh, which rely on content contributed by users, to police their systems to prevent copyright infringement.

The court began its analysis with a review of certain key facts about the way the Veoh system operated, and these facts seemed to provide important context for the court's conclusions concerning whether Veoh should have DMCA immunity. Each time users began to upload a video to the veoh.com web site they were shown a message stating, "Do not upload videos that infringe copyright, are pornographic, obscene, violent, or any other videos that violate Veoh's Terms of Use."³³²³ Veoh's employees did not review user-submitted content before it became available to other users, although Veoh's system did allow it to disable access to inappropriate videos. Veoh used a number of technologies to automatically prevent copyright infringement on its system. Beginning in 2006, when Veoh disabled access to a video that

³³¹⁸ Id.

³³¹⁹ Id. at 1088 (emphasis added).

³³²⁰ Id. at 1088-89.

³³²¹ Id. at 1092.

³³²² UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099 (C.D. Cal. 2009), aff'd sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013).

³³²³ Id. at 1102.

infringed a copyright, it used hash filtering software to thereafter automatically disable access to any identical video and block any subsequently submitted duplicates. In addition, in 2007, Veoh began using the Audible Magic commercial software to filter out potentially infringing video files from being uploaded in the first instance by taking an audio fingerprint from the video files and comparing it to a database of copyright content that was protected by copyright holders like UMG. Approximately nine months later, Veoh applied the Audible Magic filter to its backlog of videos, resulting in the removal of more than 60,000 videos. Although the vast majority of allegedly infringing files had been removed in response to notices from the RIAA (acting as UMG Recording's agent) and the Audible Magic software, several hundred other allegedly infringing files that the Audible Magic filter had failed to identify as infringing remained on the system.³³²⁴

The court then turned to analysis of each of the requirements of the Section 512(c) safe harbor. Addressing first the requirement that Veoh act expeditiously to remove infringing content upon obtaining either actual knowledge or awareness of facts and circumstances from which infringing activity is apparent, the court ruled that UMG had failed to rebut Veoh's showing that when it acquired knowledge of allegedly infringing material – whether from DMCA notices, informal notices, or other means – it expeditiously removed such material. Citing the Ninth Circuit's CCBill decision, the court noted that the DMCA notification procedures place the burden of policing copyright infringement by identifying potentially infringing material and adequately documenting infringement squarely on the copyright owner. The court noted that CCBill further taught that if investigation of facts and circumstances is required to identify material as infringing, then those facts and circumstances are not “red flags” of infringement.³³²⁵ The court concluded: “In light of the principles articulated in *CCBill* that the burden is on the copyright holder to provide notice of allegedly infringing material, and that it takes willful ignorance of readily apparent infringement to find a ‘red flag,’ Veoh has provided substantial evidence that it fulfilled the requirements of *section 512(c)(1)(A)*.”³³²⁶

Specifically, with respect to actual knowledge, the court rejected UMG's argument that Veoh had actual knowledge of infringement merely because it knew that it was hosting an entire category of content – music – that was subject to copyright protection. The court found that if this were the standard for actual knowledge, the Section 512(c) safe harbor would be a dead letter because vast portions of content on the Internet are eligible for copyright protection. Nor did Veoh's automatic tagging of more than 240,000 videos with the label “music video” give it actual knowledge that such videos were infringing. The court also rejected UMG's argument that the RIAA's DMCA notices gave Veoh notice of infringement beyond the specific materials that the RIAA identified because the notices listed artists who made the materials. UMG argued that Veoh should have sought out actual knowledge of other infringing videos by searching its system for all videos by the artists identified in the RIAA notices, because a list of artist names was equivalent to a representative list of allegedly infringing works, which the DMCA allows the

³³²⁴ Id. at 1102-04.

³³²⁵ Id. at 1107-08.

³³²⁶ Id. at 1108.

copyright holder to supply. The court ruled that providing names of artists is not the same as a representative list of works. An artist's name is not information reasonably sufficient to permit a service provider to locate allegedly infringing material. Accordingly, the court concluded that UMG had not provided evidence establishing that Veoh failed to act expeditiously whenever it had actual notice of infringement, whether from DMCA notices or other sources of information.³³²⁷

With respect to Veoh's awareness of facts or circumstances from which infringing activity was apparent under the "red flag" test, the court rejected UMG's argument that Veoh was ineligible for the safe harbor because its founders, employees, and investors knew that widespread infringement was occurring on the Veoh system. The court held that, even if this were true and undisputed, UMG had cited no case holding that a service provider's general awareness of infringement, without more, is enough to preclude application of Section 512(c), and such a holding would be contrary to Congress' intent that the DMCA safe harbors facilitate the robust development of world-wide expansion of electronic commerce, communications, and research in the digital age.³³²⁸

The court also rejected UMG's contention that Veoh avoided gaining knowledge of infringement by delaying implementation of the Audible Magic fingerprinting system for a couple of years after its commercial availability:

UMG has not established that the DMCA imposes an obligation on a service provider to implement filtering technology at all, let alone technology from the copyright holder's preferred vendor or on the copyright holder's desired timeline. Moreover, it is undisputed that Veoh did take steps to implement filtering technology before it implemented the Audible Magic system that UMG prefers, by using "hash" filtering and by attempting to develop its own filtering software. UMG dismisses hash filtering as "highly ineffectual," but that it proved deficient and that Veoh turned to Audible Magic does not negate Veoh's showing of good faith efforts to avoid or limit storage of infringing content.³³²⁹

Accordingly, the court concluded that Veoh had shown that it was not aware of "red flags," notwithstanding its knowledge of the general proposition that infringing material was often uploaded to web sites, and UMG had failed to present evidence to the contrary.³³³⁰

The court then turned to Section 512(c)'s requirement that the service provider not receive a financial benefit directly attributable to infringing activity that the service provider has the right and ability to control. The court first observed that, because the capacity to control and remove material are features that a service provider that stores content on its system must

³³²⁷ Id. at 1108-10.

³³²⁸ Id. at 1111.

³³²⁹ Id. at 111-12.

³³³⁰ Id. at 1112.

have in order to implicate the Section 512(c) safe harbor at all, those facts alone cannot constitute the type of control that is disqualifying. Nor could the right and ability to implement filtering software, standing alone or even along with Veoh's ability to control user's access, be the basis for ineligibility for the safe harbor.³³³¹ The court noted Section 512(m)'s provision that the safe harbors are not conditioned upon a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, and concluded:

If courts were to find that the availability of superior filtering systems or the ability to search for potentially infringing files establishes – without more – that a service provider has “the right and ability to control” infringement, that would effectively require service providers to adopt specific filtering technology and perform regular searches. That, in turn, would impermissibly condition the application of *section 512(c)* on “a service provider monitoring its service or affirmatively seeking facts indicating infringing activity.”³³³²

UMG urged the court to follow two “principles” it claimed were established by the Napster cases: (1) that the ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise, and (2) that to escape vicarious liability, the reserved right to police must be exercised to its fullest extent. The court refused, noting that if it were to adopt principle (1) from Napster it would render the statutory phrase “right and ability to control” redundant, because the ability to block infringers' access for any reason whatsoever is already a prerequisite to satisfying the predicate requirements of Section 512(i)(1)(A). And if the court were to adopt principle (2), it would run afoul of Section 512(m). Accordingly, the court ruled that, although the “direct financial benefit” standard should be the same as the common law direct financial benefit standard for vicarious infringement, the phrase “right and ability to control” should be construed to impose a higher standard of control than the common law standard for vicarious liability, and UMG had not established that Veoh met that higher standard of control.³³³³

Finally, the court turned to whether Veoh had met Section 512(i)'s requirement with respect to termination of repeat infringers. UMG contended that Veoh's termination policy was inadequate because it did not automatically terminate users who uploaded videos that were blocked by the Audible Magic filter. The court rejected this argument because however beneficial the Audible Magic technology was in helping to identify infringing material, it did not meet the standard of reliability and verifiability required by the Ninth Circuit to justify terminating a user's account. The court reasoned that, in view of the Ninth Circuit's ruling in CCBill that a notice by a copyright holder that specific material was allegedly infringing was not a sufficient basis for terminating a user because it lacked a sworn declaration that the notifier had

³³³¹ Id. at 1112-13.

³³³² Id. at 1113. The court also quoted H. Conf. Report 105-796 at 73 (Oct. 8, 1998): “Courts should not conclude that the service provider loses eligibility for limitations on liability under *section 512* solely because it engaged in a monitoring program.” Veoh, 665 F. Supp. 2d at 1113 n.19.

³³³³ Id. at 1115-16.

a good faith belief that the material was unlicensed, it stood to reason that Audible Magic’s automated filter also could not be a basis. The court noted that there was no evidence in the record of a feasible way for Veoh to verify information in Audible Magic’s database or evaluate Audible Magic’s process for compiling the database. Veoh had requested Audible Magic for contact information of copyright claimants for works identified by Audible Magic’s filter, for use in implementing a counter-notice procedure, and Audible Magic had refused. Accordingly, the court concluded that Veoh had no way of verifying the accuracy of Audible Magic’s database, and even if it did, it would be unreasonable to place that burden on Veoh.³³³⁴ “As a practical matter, when notice of a user’s alleged infringement is not reliable enough to justify terminating the user’s account, a service provider’s removal of the allegedly infringing material is sufficient evidence of compliance with the DMCA. In this case, when Veoh received notices of infringement it promptly removed the material identified.”³³³⁵

The court also rejected UMG’s argument that Veoh failed to adequately terminate repeat infringers because it did not necessarily terminate users who uploaded multiple videos that were identified in a single DMCA notice. If a single DMCA notice from the RIAA identified multiple videos uploaded by one user, Veoh sent the user a first warning. It then terminated the user’s account if the user subsequently uploaded another infringing video. The court held that this policy satisfied Section 512(i)’s requirements, and UMG had pointed to nothing in the statute, legislative history, or case law establishing that such a policy was not reasonable or appropriate. Accordingly, the court granted Veoh’s motion for summary judgment that it was entitled to the Section 512(c) safe harbor.³³³⁶

The Ninth Circuit’s Decision

On appeal, in a very significant and wide ranging opinion, the Ninth Circuit affirmed the entry of summary judgment in Veoh’s favor. The Ninth Circuit issued two opinions. The first was issued on Dec. 20, 2011,³³³⁷ before the Second Circuit’s decision in the Viacom case.³³³⁸ The Ninth Circuit’s first opinion differed in some respects from Viacom’s interpretation of Section 512(c). Because of that fact, after the Viacom decision was issued, the Ninth Circuit panel ordered additional briefing and agreed to rehear the case. It then issued a second opinion on Mar. 14, 2013³³³⁹ that cited Viacom approvingly and modified its analysis to bring it into close alignment with the Second Circuit with respect to the scope of the Section 512(c) safe harbor. The 2011 opinion was withdrawn. The analysis below will focus on the 2013 opinion, but will

³³³⁴ Id. at 1116-18.

³³³⁵ Id. at 1118.

³³³⁶ Id. at 1116-18.

³³³⁷ UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011).

³³³⁸ Viacom Int’l v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012).

³³³⁹ UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013).

note where significant changes were made from the earlier 2011 opinion in order to align with the Second Circuit.

Because the plaintiffs renewed their arguments that the automated processing performed by Veoh upon a video file uploaded by a user went beyond activities that are the subject of Section 512(c), the Ninth Circuit elaborated on the details of that processing. Upon upload, Veoh's software automatically broke down the video file into smaller 256-kilobyte "chunks," which facilitated making the video accessible to others. Veoh's software also automatically transcoded the video file into Flash 7 format because the vast majority of Internet users had software that could play videos in that format. If the user was a "Pro" user, the uploaded video file was also transcoded into Flash 8 and MPEG-4 formats, which are playable on some portable devices. Accordingly, when a Pro user uploaded a video, Veoh automatically created and retained four copies: the chunked file, the Flash 7 file, the Flash 8 file and the MPEG-4 file. None of those automated conversions affected the content of the video.³³⁴⁰

Veoh's computers also automatically extracted metadata from information users provided to help others locate the video for viewing. Users could provide a title, as well as tags or keywords that described the video, and could also select preset categories describing the video, such as "music," "faith" or "politics." The Veoh system then automatically assigned every uploaded video a "permalink," or web address, that uniquely identified the video and made it available to users. Veoh employees did not review the user-submitted video, title or tags before the video was made available. Users were able either to stream videos from the site or to download them in a "chunked" copy of the file to the user's computer, upon which software reassembled the chunks into a viewable file. The downloaded file was stored on the user's computer in a Veoh directory, which gave Veoh the ability to terminate access to the files.³³⁴¹ The technologies employed by Veoh to automatically reduce copyright infringement on its system, including hash filtering and Audible Magic, are described in the summary of the district courts decisions above.

The plaintiffs made three challenges to the district court's rulings. First, the plaintiffs argued that the alleged infringing activities did not fall within the plain meaning of "infringement of copyright by reason of the storage [of material] at the direction of a user" as required by Section 512(c)(1); second, that genuine issues of fact remained about whether Veoh had actual knowledge of infringement or was aware of facts or circumstances from infringing activity was apparent; and third, that the plaintiffs had presented sufficient evidence that Veoh received a financial benefit directly attributable to infringing activity that it had the right and ability to control. The court did not address whether Veoh adopted and reasonably implemented a repeat infringer termination policy or whether, upon notification, Veoh expeditiously removed or disabled access to infringing material as required by Section 512 (c). Although the plaintiffs

³³⁴⁰ Id. at 1011-12.

³³⁴¹ Id. at 1012.

contested those points in the district court, their only mention of them on appeal was in a footnote in their opening brief and they set forth no arguments as to those points.³³⁴²

“By reason of the storage.” Turning to the first issue, the court held that the phrase “by reason of the storage at the direction of the user” was meant to cover more than mere electronic storage lockers, and the language and structure of the statute, as well as the legislative intent that motivated its enactment, clarified that Section 512(c) encompasses the access-facilitating processes that automatically occurred when a user uploaded a video to Veoh. The court noted that the plaintiffs’ narrow reading of the “by reason of” language to be limited solely to storage activities per se would create internal statutory conflicts. By its terms, Section 512(c) presupposes that service providers will provide access to users’ stored material (they are required to disable access to such material upon a qualifying notice from the copyright holder), and it would thus contravene the statute to hold that such access disqualified Veoh from the safe harbor.³³⁴³

The court did not find persuasive the plaintiffs’ effort to reconcile the internal contradictions its reading of the statute created by positing that Congress must have meant Section 512(c) to protect only web hosting services. The court found that this theory failed to account for the reality that web hosts store user submitted materials in order to make those materials accessible to other Internet users. Thus, Section 512(c) should be interpreted to enable web hosting services to copy content and transmit it to Internet users. The court observed that the language of the statute recognizes that one is unlikely to infringe a copyright by merely storing material that no one could access, and so includes activities that go beyond storage in its language stating “the material *or an activity using the material* ... is infringing” (emphasis added) in Section 512(c)(1)(A)(i).³³⁴⁴

Accordingly, the court concluded, “Under the broader definition [of ‘service provider’] applying to § 512(c), there is no limitation on the service provider’s ability to modify user-submitted material to facilitate storage and access, as Veoh’s automatic processes do. Had Congress intended to include such a limitation, it would have said so expressly and unambiguously, as it did in the narrower definition of ‘service provider.’”³³⁴⁵

Knowledge. Turning to the second issue of knowledge requirements, the court began with an issue of statutory construction, noting that, “to be coherent, the statute must be read to have an implicit ‘and’ between § 512(c)(1)(A)(i) and (ii). We thus treat the provisions as stating that to qualify for the safe harbor, a service provider must either (1) have no actual knowledge

³³⁴² Id. at 1015 & n.5.

³³⁴³ Id. at 1015-17.

³³⁴⁴ Id. at 1018-19.

³³⁴⁵ Id. at 1019-20.

and no ‘aware[ness] of facts or circumstances from which infringing activity is apparent’ or (2) expeditiously remove or disable access to infringing material of which it knows or is aware.”³³⁴⁶

The Ninth Circuit first dealt with the issue of whether generalized knowledge of infringement on a service provider’s system is sufficient to disqualify the safe harbor. The plaintiffs contended that, because Veoh hosted a category of copyrightable content – music – for which it had no license from any major music company, it must have known this content was unauthorized, given its general knowledge that its services could be used to post infringing material, and this fact should be sufficient to demonstrate knowledge of infringement. The court rejected this argument on several grounds. First, it noted there are many music videos that could in fact legally appear on Veoh. And if merely hosting material that falls within a category of content capable of copyright protection, with the general knowledge that one’s services could be used to share unauthorized copies of copyrighted material, was sufficient to impute knowledge to services providers, the Section 512(c) safe harbor would be rendered a dead letter. Section 512(c) applies only to claims of copyright infringement, yet the fact that a service provider’s web site contained copyrightable material would remove the service provider from Section 512(c) eligibility.³³⁴⁷ For support, the Ninth Circuit pointed to the Supreme Court’s Sony decision, in which it ruled that, so long as the product distributed by a defendant that is used for copyright infringement is “capable of substantial noninfringing uses,” the Court refused to impute knowledge of infringement.³³⁴⁸

The Ninth Circuit noted that requiring specific knowledge of particular infringing activity made good sense in the context of the DMCA, which Congress enacted to foster cooperation among copyright holders and service providers in dealing with infringement on the Internet. These considerations were reflected in Congress’ decision to enact a notice and takedown protocol encouraging copyright holders to identify specific infringing material to service providers. They were also evidenced in the “exclusionary rule” that prohibits consideration of substantially deficient Section 512(c)(3)(A) notices for purposes of determining whether a service provider has actual knowledge or is aware of facts and circumstances from which infringing activity is apparent. Thus, Congress had made a considered policy determination that the DMCA notification procedures would place the burden of policing copyright infringement and identifying the potentially infringing material squarely on the owner of the copyright.³³⁴⁹

The court noted that its conclusion was bolstered by Section 512(m), which states that nothing in Section 512(c) shall be construed to condition the applicability of the safe harbor on a service provider monitoring its service or affirmatively seeking facts indicating infringing activity. The court rejected the plaintiffs’ argument that Section 512(m)’s title, “Protection of Privacy,”

³³⁴⁶ Id. at 1020 n.11.

³³⁴⁷ Id. at 1020-21. The court added a new footnote 12 that was not contained in its 2011 opinion, stating: “Proper DMCA notice under 17 U.S.C. § 512(c)(3) provides only a *claim* of infringement, and is not necessarily sufficient by itself to establish actual or ‘red flag’ knowledge.” Id. at 1021 n.12 (emphasis in the original).

³³⁴⁸ Id. at 1021 (quoting Sony Corp. of America v. Universal City Studios, Inc., 464 US. 417, 442 (1984)).

³³⁴⁹ UMG Recordings, 718 F.3d at 1021-22.

should cause the provision to be read narrowly. Even if privacy was the impetus for the provision, nothing in Section 512(m) suggested that fact should limit its application. Because the plain language of Section 512(m) is unambiguous, the heading could not limit the plain meaning of the text.³³⁵⁰

The court therefore held that merely hosting a category of copyrightable content, such as music videos, with the general knowledge that one's services could be used to share infringing material, is insufficient to meet the actual knowledge requirement under Section 512(c)(1)(A)(i). It reached the same conclusion with respect to Section 512(c)(1)(A)(ii), concluding that the district court's conception of the "red flag test" properly followed the Ninth Circuit's analysis in CCBill, which reiterated that the burden remains with the copyright holder rather than the service provider. Accordingly, the court held that Veoh's general knowledge that it hosted copyrightable material and that its services could be used for infringement was insufficient to constitute a red flag.³³⁵¹

The court then added a paragraph addressing willful blindness that was not contained in its 2011 opinion. Citing the Viacom decision, the Ninth Circuit noted that "a service provider cannot willfully bury its head in the sand to avoid obtaining such specific knowledge."³³⁵² However, the court agreed with the district court that there was no evidence that Veoh had acted in such a manner. Instead, the evidence demonstrated that Veoh promptly removed infringing material when it became aware of specific instances of infringement.³³⁵³ "Although the parties agree, in retrospect, that at times there was infringing material available on Veoh's services, the DMCA recognizes that service providers who do not locate and remove infringing materials they do not specifically know of should not suffer the loss of safe harbor protection."³³⁵⁴

The court also was not persuaded that the plaintiffs' other purported evidence of Veoh's actual or apparent knowledge of infringement warranted a trial. The plaintiffs argued that Veoh's purchase of certain search terms through the Google AdWords program demonstrated knowledge of infringing activity because some of the terms purchased, such as "50 Cent," "Avril Lavigne" and "Britney Spears," were the names of the plaintiffs' artists. The court noted that artists are not always in exclusive relationships with recording companies, and other recording companies had given Veoh permission to stream its videos by those artists. In addition, even absent such permission, companies sometimes purchase search terms they believe will lead

³³⁵⁰ Id. at 1022 & n.13.

³³⁵¹ Id. at 1022-23.

³³⁵² Id. at 1023.

³³⁵³ Id.

³³⁵⁴ Id.

potential customers to their web sites even if the terms do not describe goods or services the company actually provides.³³⁵⁵

The plaintiffs further argued that, although Veoh removed unauthorized content identified in RIAA notices, it should have taken the initiative to use search and indexing tools to locate and remove from its web site any other content by the artists identified in the notices. In addition, the plaintiffs argued that some of the videos on Veoh that had been pulled from MTV or other broadcast television stations bore information about the artist, song title and record label, and Veoh should have used this information to find and remove unauthorized videos. The court rejected these arguments, noting that such a requirement would conflict with Section 512(m) and CCBill's refusal to impose investigative duties on service providers.³³⁵⁶

Nor were news articles discussing the availability of copyrighted materials on Veoh, including one reporting that Veoh had been among the least aggressive video sharing sites in fighting copyrighted content, sufficient to charge Veoh with the knowledge required to disqualify the safe harbor. The DMCA's detailed notice and takedown procedure assumes that, from time to time, material belonging to someone else ends up on service providers' web sites, and establishes a process for ensuring its prompt removal. If awareness of news reports discussing this general problem were enough to remove the safe harbor, the notice and takedown procedures would make little sense and the safe harbors would be effectively nullified.³³⁵⁷

Significantly, however, the court left open the possibility that notifications of infringement from third parties other than the copyright owner might be sufficient to establish a red flag. The plaintiffs submitted evidence of emails sent to Veoh executives and investors by copyright holders and users identifying infringing content. One email, sent by the CEO of Disney, a major copyright holder, to Michael Eisner, a Veoh investor, stated that the movie *Cinderella III* and various episodes from the television show *Lost* were available on Veoh without Disney's authorization.³³⁵⁸ "If this notification had come from a third party, such as a Veoh user, rather than from a copyright holder, it might meet the red flag test because it specified particular infringing material. As a copyright holder, however, Disney is subject to the notification requirements in § 512(c)(3), which this informal email failed to meet."³³⁵⁹ Accordingly, the deficient notice could not be considered in determining whether Veoh had actual or red flag knowledge.

The court noted that, even if the email could have created actual or red flag knowledge, Eisner's email in response assured Disney that he would instruct Veoh to take it down, and Eisner copied Veoh's founder to ensure this happened right away. The plaintiffs also pointed to an email from

³³⁵⁵ Id.

³³⁵⁶ Id. at 1023-24.

³³⁵⁷ Id. at 1024-25.

³³⁵⁸ Id.

³³⁵⁹ Id.

a Veoh user whose video was rejected for containing infringing content. Upset that Veoh would not post his unauthorized material, he stated that he had seen plenty of other infringing material on the site, and identified another user who he said posted infringing content.³³⁶⁰ The court observed:

It is possible that this email would be sufficient to constitute a red flag under § 512(c)(1)(A)(ii), even though it would not qualify as sufficient notice from a copyright holder under § 512(c)(3). But even assuming that is so, UMG has not specifically alleged that Veoh failed to expeditiously remove the infringing content identified by the user's email, or that the content at issue was owned by UMG. Accordingly, this too fails to create a genuine issue of material fact regarding Veoh's knowledge of infringement.³³⁶¹

The court did not credit UMG's contention that the district court conflated the actual knowledge and red flag awareness tests. A user email informing Veoh of material that appeared to the user to be infringing and specifying its location provided a good example of the distinction.³³⁶² "Although the user's allegations would not give Veoh actual knowledge under § 512(c)(1)(A)(i), because Veoh would have no assurance that a third party who does not hold the copyright in question could know whether the material was infringing, the email could act as a red flag under § 512(c)(1)(A)(ii) provided its information was sufficiently specific."³³⁶³

The court, in a new paragraph not contained in its 2011 opinion, then adopted the Second Circuit's holding in Viacom establishing the grounds for distinction between actual and red flag knowledge by quoting the following passage from the Viacom opinion:

The difference between actual and red flag knowledge is ... between a subjective and an objective standard. In other words, the actual knowledge provision turns on whether the provider actually or "subjectively" knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement "objectively" obvious to a reasonable person. The red flag provision, because it incorporates an objective standard, is not swallowed up by the actual knowledge provision under our construction of the § 512(c) safe harbor. Both provisions do independent work, and both apply only to specific instances of infringement.³³⁶⁴

³³⁶⁰ Id. at 1025.

³³⁶¹ Id.

³³⁶² Id.

³³⁶³ Id.

³³⁶⁴ Id. (quoting Viacom, 676 F.3d at 31 (2d Cir. 2012)).

In conclusion, while the Ninth Circuit agreed that there is a distinction between actual and red flag knowledge, it held that UMG had not created a genuine issue of material fact as to whether Veoh had either kind of knowledge in this case.³³⁶⁵

Right and Ability to Control. Turning to the third issue on appeal, the Ninth Circuit concluded that the district court correctly determined that Veoh did not have the necessary right and ability to control infringing activity and thus remained eligible for safe harbor protection. This portion of the Ninth Circuit’s opinion was substantially revised from its 2011 opinion.

The 2011 Opinion. In its 2011 opinion, the Ninth Circuit (as did the district court) had imported a knowledge requirement into the right and ability to control requirement. The earlier opinion had noted that a service provider may, as a general matter, have the legal right and necessary technology to remove infringing content, but until it becomes aware of *specific* unauthorized material, it cannot exercise its power or authority over the specific infringing item and therefore could not have the kind of ability to control infringing activity the statute contemplates. The 2011 opinion bolstered its reasoning by pointing again to Section 512(m), which it found to cut against a holding urged by the plaintiffs that Veoh’s general knowledge that infringing material could be uploaded to its site triggered an obligation to exercise control by policing its services.³³⁶⁶ “We are not persuaded by UMG’s suggestion that Congress meant [Section 512(m)’s] limitation on the duty to monitor to apply only to service providers who do not receive a direct financial benefit under *subsection (b)*. Rather we conclude that a service provider must be aware of specific infringing material to have the ability to control that infringing activity within the meaning of § 512(C)(1)(B). Only then would its failure to exercise its ability to control deny it a safe harbor.”³³⁶⁷

Summarizing its holding, the court’s 2011 opinion stated: “[W]e hold that the ‘right and ability to control’ under § 512(c) requires control over specific infringing activity the provider knows about. A service provider’s general right and ability to remove materials from its services is, alone, insufficient. Of course, a service provider cannot willfully bury its head in the sand to avoid obtaining such specific knowledge. ... [T]he DMCA recognizes that service providers who are not able to locate and remove infringing materials they do not specifically know of should not suffer the loss of safe harbor protection.”³³⁶⁸ The court contrasted this more specific form of “right and ability to control” under the DMCA with that of the broader standard for common law vicarious liability, which can be met by merely having the general ability to locate infringing material and terminate users’ access, as in the Napster case.³³⁶⁹ The court did not elaborate in

³³⁶⁵ UMG Recordings, 718 F.3d at 1026.

³³⁶⁶ 667 F.3d at 1041-42.

³³⁶⁷ Id. at 1042.

³³⁶⁸ Id. at 1043.

³³⁶⁹ Id.

any way on what might constitute willfully burying one's head in the sand to avoid obtaining specific knowledge.

The 2013 Opinion. The Ninth Circuit's 2013 opinion eliminated the 2011 opinion's holding that the right and ability to control requirement also depends on knowledge of specific infringing activity, and deleted the language quoted in the two previous paragraphs above. The Second Circuit in Viacom had expressly disagreed with this formulation of the right and ability to control requirement:

[I]mporting a specific knowledge requirement into § 512(c)(1)(B) renders the control provision duplicative of § 512(c)(1)(A). Any service provider that has item-specific knowledge of infringing activity and thereby obtains financial benefit would already be excluded from the safe harbor under § 512(c)(1)(A) for having specific knowledge of infringing material and failing to effect expeditious removal. No additional service provider would be excluded by § 512(c)(1)(B) that was not already excluded by § 512(c)(1)(A).³³⁷⁰

The Ninth Circuit was apparently persuaded by this criticism, because in its 2013 opinion, as elaborated below, the Ninth Circuit adopted the Second Circuit's view that the right and ability to control requires something less than item-specific knowledge but "something more" than the general ability to locate infringing material and terminate access.

In its 2013 opinion, the Ninth Circuit began its analysis by addressing UMG's argument that Section 512(c) should be interpreted as the court did in the common law vicarious liability context in the Napster case. The Ninth Circuit noted that the Viacom case rejected that reading, and the Ninth Circuit said it too was not persuaded for several reasons. First, Section 512(c) nowhere mentions the term "vicarious liability." Although it uses a set of words that has sometimes been used to describe common law vicarious liability, the language used in the common law standard is loose and has varied. Second, Section 512(c) presumes that service providers have the sort of control UMG argued satisfied the right and ability to control requirement – namely, the ability to remove or disable access to infringing material. The court concluded that Congress could not have intended for a service provider to lose immunity under the safe harbors because it engaged in acts that are specifically required by the DMCA. The court also noted that Napster was decided after the DMCA was enacted, so Congress could not have intended to codify Napster's precise application upon which UMG was relying. Third, the court pointed to three legislative history reports of the DMCA where Congress stated explicitly that the DMCA was intended to protect qualifying service providers from liability for all monetary relief for direct, vicarious and contributory infringement, so it would be illogical to read Section 512(c) as entirely coextensive with common law vicarious liability standards.³³⁷¹

³³⁷⁰ Viacom, 676 F.3d at 36.

³³⁷¹ UMG Recordings, 718 F.3d 1026-28.

The court noted that its reading of Section 512(c)(1)(B) was reinforced by the fact that the statute would be internally inconsistent in other respects were it to interpret the right and ability to control language as UMG urged. First, Section 512(m)'s provision that the safe harbors are not conditioned on the service provider monitoring its service for infringing activity cut against holding Veoh's general knowledge that infringing material could be uploaded to its site triggered an obligation to police its services to the fullest extent possible, as required in Napster. The Ninth Circuit also noted that it had held in the CCBill case that Section 512(c) imposes no investigative duties on service providers and places the burden of policing copyright infringement squarely on the owners of the copyright. And CCBill had not suggested that Congress meant the limitation on the duty to monitor to apply only to service providers who do not receive a direct financial benefit under Section 512(c)(1)(B).³³⁷²

The Ninth Circuit therefore concluded:

In light of the DMCA's language, structure, purpose and legislative history, we are compelled to reject UMG's argument that the district court should have employed *Napster's* vicarious liability standard to evaluate whether Veoh had sufficient "right and ability to control" infringing activity under § 512(c). Although in some cases service providers subject to vicarious liability will be excluded from the § 512(c) safe harbor, in others they will not. As we are unpersuaded by UMG's argument, we conclude instead that whereas the vicarious liability standard applied in *Napster* can be met by merely having the general ability to locate infringing material and terminate users' access, § 512(c) requires "something more," *Cybernet Ventures*, 213 F. Supp. 2d at 1181 (internal quotation marks omitted); see *Napster*, 239 F.3d at 1024.³³⁷³

In specifying what abilities could constitute "something more," the Ninth Circuit indicated agreement with the Second Circuit and held that, in order to have the right and ability to control, a service provider must "exert[] substantial influence on the activities of users."³³⁷⁴ Such "substantial influence" may include, as the Second Circuit suggested, high levels of control over activities of users (as in the *Cybernet Ventures* case, where the service provider exerted a high degree of control over user activity by instituting a monitoring program that provided participating sites with detailed instructions concerning layout, appearance, and content) or purposeful conduct (such as the inducement found in the *Grokster* case).³³⁷⁵

Applying this standard, the Ninth Circuit agreed with the district court that "(a) the allegedly infringing *material* resided on Veoh's system; (b) Veoh had the ability to remove such material; (c) Veoh could have implemented, and did implement, filtering systems; and (d) Veoh

³³⁷² *Id.* at 1029.

³³⁷³ *Id.* at 1029-30.

³³⁷⁴ *Id.* at 1030 (quoting *Viacom*, 676 F.3d at 38).

³³⁷⁵ *UMG Recordings*, 718 F.3d at 1030.

could have searched for potentially infringing content.”³³⁷⁶ The court concluded, however, that these facts were not equivalent to the activities found to constitute substantial influence in Cybernet Ventures or Grokster. Nor had UMG in its initial or supplemental briefing pointed to other evidence raising a genuine issue of material fact as to whether Veoh’s activities involved something more than the ability to remove or block access to materials posted on its web site.³³⁷⁷

Accordingly, the Ninth Circuit concluded that Veoh met all the Section 512(c) requirements and affirmed the entry of summary judgment in its favor.³³⁷⁸ The court also ruled that the Veoh investor defendants, who could not claim DMCA protection, could not be liable as secondary infringers, even if Veoh were found to be liable, in the absence of evidence that they controlled Veoh’s operations.³³⁷⁹

m. Perfect 10 v. Amazon

In Perfect 10, Inc. v. Amazon.com, Inc.,³³⁸⁰ Perfect 10 sought to hold Amazon’s subsidiary A9, which operated the A9 search engine that enabled searching of content on Amazon.com and other sources, contributorily liable for infringing postings of Perfect 10’s copyrighted photos. A9 moved for summary judgment under the Section 512(c) safe harbor on the ground that it was undisputed that Perfect 10 sent its DMCA notices to Amazon rather than A9. A9 had designated its own copyright agent in Palo Alto with the Copyright Office. The Copyright Office designation included, in lieu of an email address for the agent, the URL of an online DMCA complaint form.³³⁸¹ Meanwhile, on Amazon’s web site, Amazon’s “Notice and Procedure for Making Claims of Copyright Infringement” instructed users to contact Amazon’s copyright agent in Seattle for notifying Amazon “and its affiliates” of copyright infringement. The designation Amazon filed with the Copyright Office listed a number of Amazon-owned entities as “alternative names of service provider” but A9 was not among the listed entities.³³⁸²

Perfect 10’s President, Dr. Zada, sent a letter to Amazon’s copyright agent concerning alleged infringements in the search results of A9’s search engine. Amazon’s corporate counsel, Karen Ressmeyer, called Dr. Zada and informed him that Google, not Amazon or A9, provided the search results and there was nothing Amazon could do about the complaints. After receiving several additional letters from Zada alleging infringements on A9, Ressmeyer contacted Google herself and, at Google’s suggestion, forwarded Zada’s letters to Google. She informed Zada of this fact in a letter, which she copied to Jonathan Leblang, the individual whom A9 had identified

³³⁷⁶ Id. (emphasis in the original).

³³⁷⁷ Id.

³³⁷⁸ Id. at 1031.

³³⁷⁹ Id. at 1031-33.

³³⁸⁰ 2009 U.S. Dist. LEXIS 42341 (C.D. Cal. May 12, 2009).

³³⁸¹ Id. at *2 & *4-5.

³³⁸² Id. at *5-6.

as its copyright agent in its filing at the Copyright Office. Despite all of his correspondence with Ressmeyer, Amazon never told Zada that he had to send his notices of infringement to A9 directly. No one at Amazon told him that the notices were not being forwarded to A9 or that it was not sufficient to send them to Amazon.³³⁸³

Perfect 10 argued that A9 was not entitled to the safe harbor because it had actual knowledge of infringement by virtue of the fact that it did in fact receive Perfect 10's DMCA notices. In part, Perfect 10 relied on post-litigation notices it sent to A9's copyright agent. The court ruled that the post-litigation instances of A9 receiving information of claimed infringements did not constitute notification under Section 512(c)(3) with respect to pre-litigation infringements claimed in the original complaint. Perfect 10 also cited Ressmeyer's letter to Zada that was copied to A9's copyright agent Leblang. The court rejected this basis also, noting that the letter did not indicate that Amazon forwarded any DMCA notices to A9 and did not provide any information about the infringing material, so the letter alone did not establish either that A9 received any of Perfect 10's notices or that it had actual knowledge of specific infringing activities available using its system.³³⁸⁴

Perfect 10 argued that Amazon should be equitably estopped from asserting that Perfect 10 improperly sent its notices to Amazon because the Conditions of Use posted on Amazon's site allegedly instructed copyright owners to send DMCA notices regarding its affiliates directly to Amazon. The court rejected this argument, noting that nowhere in the Conditions of Use did Amazon purport to include A9 among its affiliates and Amazon's filing with the Copyright Office identifying the subsidiary entities for which Amazon's copyright agent would accept complaints did not include A9.³³⁸⁵

Perfect 10 further argued that Amazon was the proper recipient of the notices because the infringing activity took place through the A9 search box that was on the Amazon web site. The court rejected this argument, holding that the presence of the search box on Amazon's web site did not make Amazon the proper recipient because A9 had designated its own copyright agent and Zada knew that A9 was a separate corporation entity. Perfect 10 also contended that Amazon was obligated to notify A9 of the alleged infringements because it owned and hosted A9. The court also rejected this argument, noting Perfect 10 had cited no authority that would require one OSP, by virtue of its ownership or hosting of another OSP, to pass along a DMCA notice, where the two OSPs were distinct corporate entities and each had properly designated its own copyright agent.³³⁸⁶

Lastly, Perfect 10 argued that A9 had failed to comply fully with the requirements of Section 512(c)(2) in designating a copyright agent because A9 had not provided an email address

³³⁸³ Id. at *6-10.

³³⁸⁴ Id. at *13-15.

³³⁸⁵ Id. at *15-16.

³³⁸⁶ Id. at *17-18.

for its copyright agent, but rather a URL for A9's online complaint form. The court held that this departure from the specific requirements of Section 512(c)(2) was inconsequential, and there was no genuine dispute that the Copyright Office designation enabled anyone who saw it to contact A9's designated agent, through mail, fax, telephone, or the online complaint form. Accordingly, the court ruled that A9 was entitled to a safe harbor under Section 512(c), and granted A9's motion for summary judgment as to contributory copyright infringement based on that safe harbor.³³⁸⁷

n. Louis Vuitton v. Akanoc Solutions

In Louis Vuitton Malletier, S.A. v. Akanoc Solutions, Inc.³³⁸⁸ the defendants operated hosting services for a number of web sites overseas from which counterfeit Louis Vuitton merchandise could be purchased. The plaintiff brought claims for direct and contributory infringement of its copyrights. A jury found the defendants liable for willful contributory infringement and awarded statutory damages, and found that the defendants were not entitled to the safe harbors of the DMCA. After the verdict, the defendants filed a motion for JMOL with respect to the claims.³³⁸⁹ With respect to the DMCA safe harbor, the court found that the jury had adequate evidence for denying the applicability of the Section 512(c) safe harbor. The defendants did not designate an agent with the Copyright Office until about four months after the lawsuit was filed, so at a minimum they would not be able to claim protection of the safe harbors prior to designating an agent. In addition, the evidence that the defendants had reasonably implemented a policy to terminate repeat infringers was limited, at best. For example, the designated agent for the defendants testified that he did not understand the DMCA's requirements as to maintaining or implementing the required policy. Other evidence indicated that the defendants had not terminated certain repeat offenders. Accordingly the court concluded that the jury had sufficient evidence to find for the plaintiff on the issue of the applicability of the safe harbor provisions of the DMCA.³³⁹⁰

o. Viacom v. YouTube

In Viacom Int'l v. YouTube, Inc.,³³⁹¹ the plaintiffs sought to hold YouTube and its owner Google secondarily liable for the postings by users of copyrighted videos owned by the plaintiffs. YouTube asserted the DMCA safe harbor under Section 512(c). Each side moved for summary judgment in the district court.

The District Court's Decision

³³⁸⁷ Id. at *20-23.

³³⁸⁸ 2010 U.S. Dist. LEXIS 85266 (N.D. Cal. Mar. 19, 2010), aff'd in part & rev'd in part on other grounds, 658 F.3d 936 (9th Cir. 2011).

³³⁸⁹ Id. at *1-2.

³³⁹⁰ Id. at *24.

³³⁹¹ 718 F. Supp. 2d 514 (S.D.N.Y. 2010), aff'd in part & rev'd in part, 676 F.3d 19, 26 (2d Cir. 2012).

Interestingly, in its opinion, the district court noted that from the plaintiffs' submissions on the motion, a jury could find that the defendants not only were generally aware of, but welcomed, copyright-infringing material being placed on their web site.³³⁹² Thus, according to the court, "the critical question is whether the statutory phrases 'actual knowledge that the material or an activity using the material on the system or network is infringing,' and 'facts or circumstances from which infringing activity is apparent' in § 512(c)(a)(A)(i) and (ii) mean a general awareness that there are infringements (here, claimed to be widespread and common), or rather mean actual or constructive knowledge of specific and identifiable infringements of individual items."³³⁹³

The court first quoted extensively from the legislative history of the DMCA safe harbors, then observed that the "tenor of the foregoing provisions is that the phrases 'actual knowledge that the material or an activity' is infringing, and 'facts or circumstances' indicating infringing activity, describe knowledge of specific and identifiable infringements of particular individual items. Mere knowledge of prevalence of such activity in general is not enough."³³⁹⁴ The court then reviewed existing case law on the Section 512(c) safe harbor and found it to support a similar conclusion: "if a service provider knows (from notice from the owner, or a 'red flag') of specific instances of infringement, the provider must promptly remove the infringing material. If not, the burden is on the owner to identify the infringement. General knowledge that infringement is 'ubiquitous' does not impose a duty on the service provider to monitor or search its service for infringements."³³⁹⁵

The court rejected the plaintiffs' heavy reliance on the Supreme Court's Grokster case, finding that case's explication of the more general law of contributory liability, and its application to peer-to-peer filing sharing networks (which the court observed are not covered by the DMCA Section 512(c) safe harbor), to be of little applicability in the instant case.³³⁹⁶ Said the court:

The Grokster model does not comport with that of a service provider who furnishes a platform on which its users post and access all sorts of materials as they wish, while the provider is unaware of its content, but identifies an agent to receive complaints of infringement, and removes identified material when he learns it infringes. To such a provider, the DMCA gives a safe harbor, even if otherwise he would be held as a contributory infringer under the general law. In this case, it is uncontroverted that when YouTube was given the notices, it removed the material. It is thus protect "from liability

³³⁹² Id. at 518.

³³⁹³ Id. at 519.

³³⁹⁴ Id. at 523.

³³⁹⁵ Id. at 525.

³³⁹⁶ Id. at 525-26.

for all monetary relief for direct, vicarious and contributory infringement” subject to the specific provisions of the DMCA. Senate Report at 40, House Report at 50.³³⁹⁷

The court then rejected a number of other arguments made by the plaintiffs. First, the plaintiffs asserted that the replication, transmittal and display of videos on YouTube did not constitute infringement “by reason of the storage at the direction of a user of material” on the site. The court found that the argument confined the word “storage” too narrowly to meet the statute’s purpose. The court noted that the definition of “service provider” protected by the safe harbor includes an entity “offering the transmission, routing, or providing of connections for digital online communications.”³³⁹⁸ The court inferred from this definition that “the provision of such services, access, and operation of facilities were meant to be within the safe harbor when they flow from the material’s placement on the provider’s system or network: it is inconceivable that they are left exposed to be claimed as unprotected infringements.”³³⁹⁹ The court agreed with the ruling in Io Group v. Veoh³⁴⁰⁰ that “by reason of” in the Section 512(c) safe harbor means “as a result of” or “something that can be attributed to.”³⁴⁰¹

Second, the court rejected the plaintiffs’ argument that YouTube did not qualify for the safe harbor because it derived a financial benefit directly attributable to the infringing activity, over which it had the right and ability to control. The court held that the “right and ability to control” the activity requires knowledge of it, which must be item-specific. A service provider must know of a specific infringement before the service provider can control it.³⁴⁰² Under the court’s logic with respect to this knowledge requirement, so long as YouTube acted to take down infringing material once it received specific knowledge of it (including through red flags), the financial benefit prong would not provide an independent basis on which to disqualify the safe harbor.

Third, the court rejected a number of other smaller bases asserted by the plaintiffs as disqualifying YouTube from the safe harbor:

– The court found YouTube’s repeat infringer policy to be reasonable when it counted as only one strike against a user both a single DMCA take-down notice identifying multiple videos uploaded by the user and multiple take-down notices identifying videos uploaded by the user received by YouTube within a two-hour period.³⁴⁰³

³³⁹⁷ Id. at 526.

³³⁹⁸ Id. at 526.

³³⁹⁹ Id. at 526-27.

³⁴⁰⁰ 586 F. Supp. 2d 1132, 1148 (N.D. Cal. 2008).

³⁴⁰¹ YouTube, 718 F. Supp. 2d at 527.

³⁴⁰² Id.

³⁴⁰³ Id. at 527-28.

– The court also found reasonable YouTube’s treatment of takedowns resulting from its “Claim Your Content” system. YouTube used Audible Magic technology to remove an offending video automatically if it matched some portion of a reference video submitted by a copyright owner who had designated the service. It also removed a video if the rightsholder operated a manual function after viewing the infringing video. YouTube assigned strikes only when the rightsholder manually requested the video to be removed. In addition, the court found YouTube’s initial hesitation in counting manual removals as strikes to be reasonable. YouTube’s six month delay in counting such strikes was needed to monitor the system’s use by rightsholders, and for engineering work to assure that strikes would be assigned accurately.³⁴⁰⁴

Finally, in an important ruling, the court rejected the plaintiffs’ complaint that YouTube removed only the specific clips identified in DMCA notices, and not other clips which infringed the same works. The plaintiffs pointed to the provision in Section 512(c)(3)(A)(ii) that permits a representative list of infringing works at the site. The court ruled that this “representative list” provision would eviscerate the required specificity of notice if it were construed to mean a merely generic description (such as “all works by Gershwin”) would be adequate without also giving the works’ location at the site, and would put the provider to the factual search forbidden by Section 512(m).³⁴⁰⁵ “Although the statute states that the ‘works’ may be described representatively, 512(c)(3)(A)(ii), the subsection which immediately follows requires that the identification of the infringing material that is to be removed must be accompanied by ‘information reasonably sufficient to permit the service provider to locate the material.’”³⁴⁰⁶

Accordingly, the court granted summary judgment to the defendants that they qualified for the Section 512(c) safe harbor.³⁴⁰⁷

The Second Circuit’s Decision

On appeal, the Second Circuit affirmed in part and reversed in part in a very important opinion. The Second Circuit concluded that the district court correctly held that the Section 512(c) safe harbor requires knowledge or awareness of specific infringing activity, but vacated the order granting summary judgment because a reasonable jury could find that YouTube had actual knowledge or awareness of specific infringing activity on its web site.³⁴⁰⁸

The Second Circuit turned first to the applicability of the Section 512(c) safe harbor.³⁴⁰⁹ The court noted that, with respect to applicability of the safe harbor, the most important question on appeal was whether the safe harbor requires actual knowledge or awareness of

³⁴⁰⁴ Id. at 528.

³⁴⁰⁵ Id. at 528-29.

³⁴⁰⁶ Id. at 529.

³⁴⁰⁷ Id.

³⁴⁰⁸ Viacom Int’l, Inc. v. YouTube, Inc., 676 F.3d 19, 26 (2d Cir. 2012).

³⁴⁰⁹ Id. at 28.

facts or circumstances indicating specific and identifiable infringements, as opposed to merely a general awareness that infringing activity is or may be present on the web site. The court concluded that the text of Section 512(c) requires knowledge or awareness of specific infringing activity. The court noted that the nature of the removal obligation in Section 512(c)(1)(A) itself contemplates knowledge or awareness of specific infringing material, because expeditious removal would be possible only if the service provider knows with particularity which items to remove.³⁴¹⁰ “Indeed, to require expeditious removal in the absence of specific knowledge or awareness would be to mandate an amorphous obligation to ‘take commercially reasonable steps’ in response to a generalized awareness of infringement. Such a view cannot be reconciled with the language of the statute, which requires ‘expeditious[]’ action to remove or disable ‘*the material*’ at issue.”³⁴¹¹

The court rejected Viacom’s argument that the “red flag” provision of Section 512(c) must require less specificity of knowledge than the actual knowledge provision in order to give rise to a duty to act, else the red flag provision would be superfluous. The court concluded that requiring actual knowledge or awareness of specific instances of infringement does not render the red flag superfluous, because the phrase “actual knowledge” in Section 512(c)(1)(A)(i) is frequently used to denote subjective belief, whereas the language of “facts or circumstances” appearing in Section 512(c)(1)(A)(ii) is often used to denote an objective reasonableness standard.³⁴¹²

The difference between actual and red flag knowledge is thus not between specific and generalized knowledge, but instead between a subjective and an objective standard. In other words, the actual knowledge provision turns on whether the provider actually or “subjectively” knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement “objectively” obvious to a reasonable person. The red flag provision, because it incorporates an objective standard, is not swallowed up by the actual knowledge provision under our construction of the § 512(c) safe harbor. Both provisions do independent work, and both apply only to specific instances of infringement.³⁴¹³

Accordingly, the Second Circuit affirmed “the District Court’s holding that actual knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement will disqualify a service provider from the safe harbor.”³⁴¹⁴

Applying these standards, the court next turned to whether the district court had correctly granted summary judgment based on the facts of the case. The plaintiffs cited

³⁴¹⁰ *Id.* at 30.

³⁴¹¹ *Id.* at 30-31 (emphasis in original) (citations omitted).

³⁴¹² *Id.* at 31.

³⁴¹³ *Id.*

³⁴¹⁴ *Id.* at 32.

evidence that YouTube employees conducted web site surveys and estimated that 75-80% of all YouTube streams contained copyrighted material, and that Credit Suisse, acting as financial advisor to Google, estimated that more than 60% of YouTube's content was "premium" copyrighted content and that only 10% of the premium content was authorized. The court held that such estimates were insufficient, standing alone, to create a triable issue of fact as to whether YouTube actually knew, or was aware of facts or circumstances that would indicate, the existence of particular instances of infringement.³⁴¹⁵

The plaintiffs also relied upon internal YouTube communications that referred to particular clips or groups of clips, citing an email from the director of video partnerships for Google and YouTube, requesting that his colleagues calculate the number of daily searches for the terms "soccer," "football," and "Premier League" in preparation for a bid on the global rights to Premier League content. On another occasion he requested that any "clearly infringing, official broadcast footage" from a specific list of top Premier League clubs be taken down in advance of a meeting with the heads of several major sports teams and leagues. YouTube ultimately decided not to make a bid for the Premier League rights, but the infringing content allegedly remained on the web site. In addition, one of the YouTube founders prepared a report in March 2006 stating that "[a]s of today[,] episodes and clips of the following well-known shows can still be found [on YouTube]: Family Guy, South Park, MTV Cribs, Daily Show, Reno 911, [and] Dave Chapelle [sic]." He further opined that, "although YouTube is not legally required to monitor content ... and complies with DMCA takedown requests, we would benefit from *preemptively* removing content that is illegal and likely to attract criticism." He also noted that "a more thorough analysis" of the issue would be required.³⁴¹⁶

The court held that a reasonable juror could conclude from the March 2006 report that the founder knew of the presence of Viacom-owned material on YouTube, since he presumably located specific clips of the shows in question before he could announce that YouTube hosted the content "as of today." A reasonable juror could also conclude that he believed the clips he located to be infringing since he referred to them as "blatantly illegal," and that YouTube did not remove the content from the web site until "a more thorough analysis," thus exposing the company to liability in the interim. The court also pointed to other email exchanges between founder Chad Hurley and Steven Chen, in which Hurley identified specific copyrighted material that should be taken down but Chen requested that the material stay up a bit longer, in one instance suggesting that a CNN space shuttle clip remain up until "we're bigger and better known."³⁴¹⁷ Based upon this various evidence, the court concluded that the plaintiffs "may have raised a material issue of fact regarding YouTube's knowledge or awareness of specific instances of infringement."³⁴¹⁸ Accordingly, the court vacated the district court's order granting summary judgment and instructed the district court to determine on remand whether any specific

³⁴¹⁵ Id. at 32-33.

³⁴¹⁶ Id.

³⁴¹⁷ Id. at 33-34.

³⁴¹⁸ Id. at 34.

infringements of which YouTube had knowledge or awareness corresponded to the specific clips that were in suit.³⁴¹⁹

The Second Circuit next turned to an issue of first impression – the application of the common law doctrine of willful blindness in the DMCA context – raised by the plaintiffs’ argument that the district court also erred in granting summary judgment because there was evidence that YouTube was willfully blind to specific infringing activity, which should be treated as tantamount to knowledge. The court noted that, as a general matter of statutory interpretation, a statute should be interpreted to abrogate a common law principle only if the statute speaks directly to the question addressed by the common law. The DMCA provision most relevant to the abrogation inquiry, in the court’s view, was Section 512(m), which provides that safe harbor protection is not conditioned upon a service provider monitoring its service or affirmatively seeking facts indicating infringing activity.³⁴²⁰ The court noted that Section 512(m) “is incompatible with a broad common law duty to monitor or otherwise seek out infringing activity based on general awareness that infringement may be occurring.”³⁴²¹ However, that fact did not end the abrogation inquiry because willful blindness cannot be defined as an affirmative duty to monitor. The court ruled:

Because the statute does not ‘speak[] directly’ to the willful blindness doctrine, § 512(m) limits – but does not abrogate – the doctrine. Accordingly, we hold that the willful blindness doctrine may be applied, in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under the DMCA.³⁴²²

Because the district court had not expressly addressed the principle of willful blindness or its relationship to the DMCA safe harbors, the Second Circuit instructed the district court to consider on remand the fact question of whether the defendants made a deliberate effort to avoid guilty knowledge of infringement.³⁴²³

The Second Circuit then turned to the issue of the right and ability to control infringing activity. Under Section 512(c)(A)(B), a service provider loses the safe harbor if it receives a financial benefit directly attributable to the infringing activity in a case in which the service provider has the right and ability to control such activity. The Second Circuit rejected the district court’s importation of a knowledge element into the control test on the ground that the service provider must know of the particular infringement before he can control it. The court was troubled by the fact that importing a specific knowledge requirement into Section 512(c)(1)(B) would render the control provision duplicative of Section 512(C)(1)(A): “Any service provider that has item-specific knowledge of infringing activity and thereby obtains financial benefit

³⁴¹⁹ Id.

³⁴²⁰ Id. at 34-35.

³⁴²¹ Id. at 35.

³⁴²² Id.

³⁴²³ Id.

would already be excluded from the safe harbor under § 512(c)(1)(A) for having specific knowledge of infringing material and failing to effect expeditious removal.”³⁴²⁴

The Second Circuit also rejected the construction urged by the plaintiffs – that the control provision codifies the common law doctrine of vicarious copyright liability. The court noted the general rule with respect to common law codification that when Congress uses terms that have accumulated settled meaning under the common law, a court should infer, unless the statute otherwise dictates, that Congress meant to incorporate the established meaning of those terms.³⁴²⁵ The Second Circuit noted that under the common law vicarious liability standard, “[t]he ability to block infringers’ access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise.”³⁴²⁶ However, to adopt that principle in the DMCA context would render the statute internally inconsistent, because Section 512(c) actually presumes that services providers have the ability to block access to infringing material. Indeed, the safe harbor requires the services provider to remove or disable access to material once it has knowledge or awareness of infringing material. But in taking such action, the service provider would – under the plaintiffs’ proposed construction – be admitting the right and ability to control the infringing material. Thus, the prerequisite to safe harbor protection under Sections 512(c)(1)(A)(iii) & (C) would at the same time be a disqualifier under Section 512(c)(1)(B).³⁴²⁷

In view of this predicament, the Second Circuit concluded that the control provision dictates a departure from the common law vicarious liability standard, and ruled that the right and ability to control infringing activity under Section 512(c)(1)(B) requires something more than the ability to remove or block access to materials posted on a service provider’s web site. The court refused to elaborate, however, on what that “something more” might be, choosing instead simply to recite two examples of “something more” that would satisfy the control provision. First, the court cited the only court decision that as of the time had found a service provider had the right and ability to control infringing activity.³⁴²⁸ In Perfect 10, Inc. v. Cybernet Ventures, Inc.,³⁴²⁹ the district court found control where the service provider instituted a monitoring program by which user web sites received detailed instructions regarding issues of layout, appearance, and content. The service provider also forbade certain types of content and refused access to users who failed to comply with its instructions.³⁴³⁰

³⁴²⁴ Id. at 36. The Second Circuit’s reasoning seems flawed on this point, in that a service provider could obtain financial benefit from infringing activity before it became specifically aware of the infringing material and then acted to remove it.

³⁴²⁵ Id. at 36-37.

³⁴²⁶ Id. at 37 (quoting A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001)).

³⁴²⁷ Viacom, 676 F.3d at 37.

³⁴²⁸ Id. at 37-38.

³⁴²⁹ 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

³⁴³⁰ Id. at 1173.

As a second example, the Second Circuit noted that inducement of copyright infringement as enunciated in the Supreme Court’s Grokster decision, which premises liability on purposeful, culpable expression and conduct, might also rise to the level of control under Section 512(c)(1)(B).³⁴³¹ The court noted that both of its examples involve a service provider “exerting substantial influence on the activities of users, without necessarily – or even frequently – acquiring knowledge of specific infringing activity.”³⁴³² In view of its holding that the control requirement does not include a specific knowledge requirement, the Second Circuit remanded to the district court to consider in the first instance whether the plaintiffs had adduced sufficient evidence to allow a reasonable jury to conclude that YouTube had the right and ability to control the infringing activity and received a financial benefit directly attributable to that activity.³⁴³³

The Second Circuit next turned to an analysis of what activities fall within Section 512(c)’s safe harbor for infringement “by reason of the storage at the direction of a user” of material residing on the service provider’s system or network. The Second Circuit affirmed the district court’s holding with respect to three of the challenged software functions at issue – the transcoding of videos into a standard display format, the playback of videos on “watch” pages, and the “related videos” function. The court remanded for further fact finding with respect to a fourth software function, involving the third party syndication of videos uploaded to YouTube.³⁴³⁴

The court first noted that the structure of the two alternative definitions of “service provider” suggests the safe harbors of Section 512(c) do not exclude all activity that involves modification of user posted content. Specifically, although the definition of “service provider” that applies to the Section 512(a) safe harbor requires that there be no modification of content of the material being transmitted by the service provider, the definition of “service provider” applicable to Section 512(c) does not contain that limitation. Accordingly, the court found it apparent that the Section 512(c) safe harbor was intended to cover more than mere electronic storage lockers. Instead, the court pointed to various previously decided safe harbor cases as establishing that the safe harbor extends to software functions performed for the purpose of facilitating access to user stored material. One of those cases had expressly considered two of the software functions challenged here – automatic transcoding and playback – and found liability arising from those functions to have occurred “by reason of the storage at the direction of a user.” The Second Circuit therefore ruled that the district court had correctly found that to exclude those automated functions from the safe harbor would eviscerate the protection afforded by Section 512(c).³⁴³⁵

³⁴³¹ Viacom, 676 F.3d at 38.

³⁴³² Id.

³⁴³³ Id.

³⁴³⁴ Id. at 38-39.

³⁴³⁵ Id. at 39.

A similar analysis applied to the “related videos” function, by which a YouTube computer algorithm identified and displayed thumbnails of clips that were related to the video selected by the user. The court rejected the plaintiffs’ argument that this practice constituted content promotion, not “access” to stored content. The record established that the related videos algorithm was fully automated and operated solely in response to user input without the active involvement of YouTube employees. The related videos function served to help YouTube users locate and gain access to material stored at the direction of other users. Because the algorithm was closely related to, and followed from, the storage itself, and was narrowly directed toward providing access to material stored at the direction of users, the Second Circuit concluded that the related videos function was protected by the Section 512(c) safe harbor.³⁴³⁶

The court then considered the syndication function, under which YouTube had transcoded a select number of videos into a format compatible with mobile devices and syndicated or licensed the videos to Verizon Wireless and other companies. The plaintiffs argued – with some force, the court noted – that business transactions do not occur at the “direction of a user” when they involve the manual selection of copyrighted material for licensing to a third party. The parties did not dispute, however, that none of the clips in suit were among the approximately 2,000 videos provided to Verizon Wireless. The court therefore held that, in order to avoid rendering an advisory opinion on the outer boundaries of the storage provision, it should remand for fact finding on the question of whether any of the clips in suit were in fact syndicated to any other third party.³⁴³⁷

Finally, the Second Circuit addressed the plaintiffs’ argument that YouTube’s repeat infringer policy was inadequate because YouTube had deliberately set up its proprietary identification tools to try to avoid identifying infringements of the plaintiffs’ works by permitting only designated “partners” to gain access to those identification tools by which YouTube would conduct network searches and identify infringing material. The court rejected this argument, noting that Section 512(m) provides that the Section 512(c) safe harbor is not conditioned on a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent such monitoring comprises a “standard technical measure” within the meaning of Section 512(i). The court noted that, while refusing to accommodate or implement a “standard technical measure” exposes a service provider to liability, refusing to provide access to mechanisms by which a service provider affirmatively monitors its own network has no such result. In this case, the plaintiffs had made no argument that YouTube’s content identification tools constituted “standard technical measures,” and YouTube could therefore not be excluded from the safe harbor by dint of a decision to restrict access to its proprietary search mechanisms.³⁴³⁸

The District Court’s Decision on Remand

³⁴³⁶ *Id.* at 39-40.

³⁴³⁷ *Id.* at 40.

³⁴³⁸ *Id.* at 40-41.

On remand, the district court again granted summary judgment for YouTube. With respect to the issue of actual knowledge, the court noted that Viacom had recognized that it had failed to come forward with evidence establishing YouTube’s knowledge of specific clips-in-suit. Viacom argued that fact did not matter, because it was not Viacom’s burden to prove notice. Viacom argued that because YouTube was claiming the statutory defense, it had the burden of establishing each element of the defense, including the lack of knowledge or awareness of Viacom’s clips-in-suit. The court rejected this argument, noting that the DMCA places the burden of notifying the service provider of infringements upon the copyright owner, and because Viacom had acknowledged that it lacked the kind of evidence that would allow a clip-by-clip assessment of actual knowledge, Viacom had failed to show actual knowledge on YouTube’s part.³⁴³⁹

With respect to the issue of willful blindness, the district court noted the Second Circuit had recognized that willful blindness is not the same as an affirmative duty to monitor. From the Second Circuit’s discussion of “red flags,” the district court concluded that under the DMCA, what disqualifies the service provider from the safe harbor is blindness to specific and identifiable instances of infringement. Here, the examples proffered by the plaintiffs to which YouTube was allegedly willfully blind gave at most information that infringements were occurring with particular works, and occasional indications of promising areas to locate and remove them. The specific locations of infringements were not supplied – at most, an area of search was identified, and YouTube was left to find the infringing clip. A memorandum submitted by one of the plaintiffs noted that infringing clips of well-known shows could still be found on YouTube at the time, but the court noted that to find them would require YouTube to locate and review over 450 clips, and Section 512(m) of the DMCA excuses YouTube from doing that search. The court therefore concluded that the plaintiffs had made no showing of willful blindness to specific infringement of the clips-in-suit.³⁴⁴⁰

Turning to whether YouTube had the right and ability to control infringing activity, the district court opined that, by its example of the extreme *Grokster* case as what might rise to the level of control under Section 512(c)(1)(B), the Second Circuit kept intact its determination that the DMCA requires actual knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement before disqualifying a service provider from the safe harbor. The district court also pointed to Ninth Circuit cases requiring high levels of control over activities of users or purposeful conduct as in *Grokster* for disqualification under the control prong.³⁴⁴¹ “But the governing principle must remain clear: knowledge of the prevalence of infringing activity, and welcoming it, does not itself forfeit the safe harbor. To forfeit that, the provider must influence or participate in the infringement.”³⁴⁴²

³⁴³⁹ Viacom Int’l Inc. v. YouTube, Inc., 940 F. Supp. 2d 110, 114-15 (S.D.N.Y. 2013).

³⁴⁴⁰ Id. at 116-17.

³⁴⁴¹ Id. at 117-18.

³⁴⁴² Id. at 118.

The plaintiffs cited evidence from prior to its acquisition by Google that allegedly established YouTube's willingness that its service be used to infringe and its ultimate editorial judgment and control over the content available on the site. Specifically, the plaintiff cited emails among YouTube founders acknowledging the need to avoid looking like a dumping ground for copyrighted material or like BitTorrent, without risking drops in site traffic and viral behavior. In particular, YouTube decided to take down whole movies, entire TV shows, nudity, porn and any death videos, but to leave up music videos, news programs, sports, commercials and comedy clips. YouTube then disabled community flagging for infringement and declined to send automated email alerts to copyright owners when illegal content was uploaded. The plaintiffs also noted that YouTube manually screened videos uploaded by participants in its Director Program and its User Partner Program, although not other users, and used hash based identification technology to prevent identical material that had been taken down from being posted again.³⁴⁴³

In response, the court observed that such evidence proved only that YouTube for business reasons placed much of the burden on the plaintiffs to search YouTube constantly for infringing content, and that is where it lies under the safe harbor. The court ruled that YouTube's decisions to restrict its monitoring efforts to certain groups of infringing clips, like its decisions to restrict access to its proprietary search mechanisms, did not exclude it from the safe harbor, regardless of their motivation. And the plaintiffs' remaining evidence of control went no further than the normal functioning of any service provider, and showed neither participation in, nor coercion of, user infringement activity.³⁴⁴⁴ The court summed up as follows:

Thus, during the period relevant to this litigation, the record establishes that YouTube influenced its users by exercising its right not to monitor its service for infringements, by enforcing basic rules regarding content (such as limitations on violent, sexual or hate material), by facilitating access to all user-stored material regardless (and without actual or constructive knowledge) of whether it was infringing, and by monitoring its site for some infringing material and assisting some content owners in their efforts to do the same. There is no evidence that YouTube induced its users to submit infringing videos, provided users with detailed instructions about what content to upload or edited their content, prescreened submissions for quality, steered users to infringing videos, or otherwise interacted with infringing users to a point where it might be said to have participated in their infringing activity.³⁴⁴⁵

Finally, the court turned to the allegations that YouTube syndicated infringing material, noting as an initial matter that the clips delivered to Verizon Wireless were not clips-in-suit. YouTube had entered into syndication agreements with Apple, Sony, Panasonic, TiVo and AT&T under which YouTube provided access to material stored on its system at the direction of users by transcoding, to a format accessible by third party mobile and similar technology, all of the

³⁴⁴³ Id. at 199-20 & n.5.

³⁴⁴⁴ Id. at 120-21.

³⁴⁴⁵ Id. at 121.

videos stored on its system. The court noted that such “syndication” served the purposes of Section 512(c) by “providing access to material stored at the direction of users,” and entailed neither manual selection nor delivery of videos. The plaintiffs argued that the critical feature of these syndication deals that took them outside the safe harbor was that they were entered into sua sponte by YouTube for its own business purposes, and not at the direction of users. The court ruled that, on the contrary, the critical feature of the transactions was not the identity of the party initiating them, but that they were steps by a service provider taken to make user-stored videos more readily accessible (without manual intervention) from its system to those using contemporary hardware. The syndication transactions were therefore protected by the Section 512(c) safe harbor.³⁴⁴⁶

In March 18, 2014 the parties announced that they had reached a settlement of the lawsuit on terms that were not made public, although it was reported that no money changed hands.³⁴⁴⁷

p. Perfect 10 v. Google

The rulings of this case with respect to the Section 512(c) safe harbor are discussed in Section III.C.6(b)(1)(ii) above.

q. Wolk v. Kodak Imaging Network

In Wolk v. Kodak Imaging Network, Inc.,³⁴⁴⁸ the plaintiff sought a preliminary injunction against the Photobucket web site preventing it from infringing on copyrights in her photographs. The plaintiff had submitted various notices to Photobucket requesting that images infringing her copyrights be taken down, some of which complied with the DMCA notice requirements and some of which did not. Where a DMCA compliant notice was submitted, Photobucket took down the allegedly infringing photo. Photobucket also had taken down photos where the plaintiff had sufficiently identified the alleged infringements, even if the notice was not DMCA compliant. Despite these removals, the plaintiff contended that more infringing photos remained on Photobucket, although she had not provided DMCA compliant notices to remove them.³⁴⁴⁹

Photobucket relied on the Section 512(c) safe harbor as a shield against the broad preliminary injunction sought by the plaintiff. The court ruled that Photobucket had satisfied all the predicate conditions of Sections 512(i) and 512(k) for the safe harbor. The plaintiff argued that her past notices of infringement also served as DMCA compliant notice of other present and

³⁴⁴⁶ Id. at 122-23.

³⁴⁴⁷ Jonathan Stempel, “Google, Viacom settle landmark YouTube lawsuit,” *Reuters* (Mar. 18, 2014), available as of Mar. 18, 2014 at <http://www.reuters.com/article/2014/03/18/us-google-viacom-lawsuit-idUSBREA2H11220140318>.

³⁴⁴⁸ 2011 U.S. Dist. LEXIS 27541 (S.D.N.Y. Mar. 17, 2011).

³⁴⁴⁹ Id. at *1-2.

future alleged infringements of the same copyrighted works posted at different times and at different locations. She contended, in essence, that Photobucket was now aware that her copyrights were being infringed on its site, and it was thereafter required to police its site to uncover current infringements and prevent future infringements, without her providing DMCA compliant notices in each instance. The court rejected this attempt to shift the burden of policing from the plaintiff to Photobucket, citing Section 512(m)(1) and several cases holding that the underlying purpose of the notice requirements of the DMCA was to place the burden of policing copyright infringement on the owner of the copyright. Without receiving notices identifying and locating each instance of infringement, Photobucket did not have actual knowledge of the infringements or awareness of facts or circumstances from which infringing activity was apparent.³⁴⁵⁰

The court also concluded that Photobucket was not disqualified from the Section 512(c) safe harbor, in that it did not have the right or ability to control the posting of infringing photos on its site and did not receive a direct financial benefit from the alleged infringing activity. The court noted that a right and ability to control may take the form of prescreening content, providing extensive advice to users regarding content, and editing user content, but Photobucket did not engage in any of such activities (and the size of its web site curtailed its ability to do so). The court rejected the plaintiff's argument that Photobucket received financial gain through its relationship with Kodak, under which it received a share of sales derived from Photobucket. The court noted that such financial gain was derived from allowing all users access to Kodak's services, not directly and specifically from allowing users to print infringing material. Accordingly, Photobucket was entitled to the Section 512(c) safe harbor, and the court denied the motion for a preliminary injunction.³⁴⁵¹

The plaintiff subsequently sought summary judgment of infringement against both Photobucket and Kodak – in Kodak's case, for its operation of the Kodak Gallery, which allowed its customers the ability to upload their personal digital photographs, create and store albums to share with family and friends, and to order prints of and products containing their digital photographs. Beginning in 2009, Photobucket and Kodak entered into an agreement that allowed Photobucket users to print images obtained from Photobucket on products available through the Kodak Gallery.³⁴⁵²

With respect to Kodak, the plaintiff sought to hold it liable for direct copyright infringement by reproducing unauthorized copies of her images on products available through the Kodak Gallery. The court rejected her claim because there was no evidence of volitional conduct on the part of Kodak required for direct liability. Specifically, the record established that the transfer of information about an order from the Kodak Gallery web site to the fulfillment vendor was done electronically through an automated computer system and that all information

³⁴⁵⁰ Id. at *4-7, *11-14.

³⁴⁵¹ Id. at *16-19, *25.

³⁴⁵² Wolk v. Kodak Imaging Networks, Inc., 840 F. Supp. 2d 724, 728, 730 (S.D.N.Y. 2012), aff'd sub nom. Wolk v. Photobucket, Inc., 569 Fed. Appx. 51 (2d Cir. 2014) (summary order).

displayed on the Kodak Gallery web site, including the simulation of products containing the Photobucket images, was done electronically. There was no dispute that any reproduction, display or transmission of the plaintiff's images by or through the Kodak Gallery web site was an automated process with no human intervention by any employee of the defendants. The fact that the plaintiff's images were copied into product simulations in addition to being transmitted to fulfillment vendors did not constitute a volitional act where the copying was automated. The court also ruled that the display of copyrighted images on the defendant's web site did not demonstrate volition either.³⁴⁵³

The court held that Photobucket was entitled to the Section 512(c) DMCA safe harbor. With respect to the threshold conditions of the safe harbor, the court found that Photobucket had an adequate policy to terminate repeat infringers. The evidence established that it had developed a policy, made available on its web site, under which copyright holders could submit a take-down notice and when Photobucket received those notices, both those that included URLs and those that did not, it acted to remove the infringing material. The court rejected the plaintiff's argument that Photobucket failed to accommodate standard technical measures because it afforded its users computer tools that allowed users to obliterate, hide or crop out the copyright watermarks on images uploaded. The court noted that the plaintiff had not suggested that Photobucket advised or encouraged its users to use the photo editing tools to circumvent the copyright notice. In any event, the court found the fact that the watermarks appeared on content on the site suggested that Photobucket did, in fact, accommodate standard technical measures. Although the plaintiff argued that the editing software interfered with standard technical measures, the court noted that it was not Photobucket, but rather users, who would use the editing tools to attempt to circumvent copyright protection measures that were already on the site. Accordingly, the editing tools did not disqualify Photobucket from safe harbor eligibility.³⁴⁵⁴

Turning to the knowledge prong, the court again rejected the plaintiff's argument that her provision of fifteen notices of infringement of nine different works was sufficient to serve as DMCA-compliant notice of any and all other unidentified alleged infringements of those nine works that might appear on the Photobucket site. The court held that notices that do not identify the specific location of the alleged infringement (such as a URL) are not sufficient to confer actual notice on the service provider. In those specific instances where the plaintiff validly notified Photobucket of infringing activity, it was undisputed that Photobucket had acted promptly to take down the infringing material. Even in instances where notices were non-compliant, Photobucket had acted to remove the material.³⁴⁵⁵

With respect to the control and financial benefit prong, the court held that the mere ability to remove or block access to materials on the web site is not sufficient to satisfy the control prong. Rather, "a right and ability to control must take the form of prescreening content,

³⁴⁵³ Id. at 742-43.

³⁴⁵⁴ Id. at 744-45.

³⁴⁵⁵ Id. at 746-47.

rendering extensive advice to users regarding content and editing user content.”³⁴⁵⁶ Here, Photobucket had not engaged in any such activity. Although the plaintiff alleged that Photobucket received a financial benefit from infringements from a profit sharing relationship with the Kodak defendants, there was no evidence indicating that either the Kodak defendants or Photobucket capitalized *specifically* because a given image a user selected to print was infringing. Rather, the defendants’ profits were derived from the service the provided, not a particular infringement. Further, Photobucket had no knowledge of which images users might select to send to the Kodak defendants to be printed, and, as such, Photobucket had no ability to control whether users requested that infringing material be printed. (The court thus seemingly grafted a knowledge element into the control prong.)³⁴⁵⁷

Next, the court ruled that Photobucket had adequately satisfied the predicate requirement of designating an agent to receive DMCA notifications. Photobucket posted contact information of its agent on its web site, including instructions to send notices to “Copyright Agent” at a listed physical address, email address, or fax. The court held that, although this contact information did not include a name or phone number, the statute mandates that the service provider provide only “substantially the following information” referenced in the statute, and by including the physical address, email address and fax number of the copyright agent, Photobucket had included sufficient information to have properly designated an agent.³⁴⁵⁸

Finally, in some final miscellaneous rulings without much elaboration in the opinion, the court held that under the provisions of Section 512(m), Photobucket had no duty to do the policing of its web site for infringements that the Plaintiff suggested, and Photobucket could not be held liable for contributory or vicarious infringement because it was entitled to the Section 512(c) safe harbor. And in any event, the evidence did not support the plaintiff’s allegation of contributory infringement because she had not demonstrated Photobucket to have acted with knowledge that it was passing along infringing images to the Kodak defendants, that it acted in concert with the Kodak defendants to infringe upon the plaintiff’s copyrights, or that it sought to encourage copyright infringement or promoted its service as a means of circumventing copyright.³⁴⁵⁹

On appeal, the Second Circuit affirmed in a short per curiam opinion, agreeing that the district court had properly granted summary judgment for substantially the reasons stated by the district court.³⁴⁶⁰ The Second Circuit rejected the plaintiff’s argument that Photobucket

³⁴⁵⁶ Id. at 747-48.

³⁴⁵⁷ Id. at 748.

³⁴⁵⁸ Id. at 748-49.

³⁴⁵⁹ Id. at 749-50.

³⁴⁶⁰ Wolk v. Photobucket, Inc., 569 Fed. Appx. 51 (2d Cir. 2014).

should have done more to police its web site for infringing material, an argument it found foreclosed by its decision in Viacom Int'l Inc. v. YouTube, Inc.³⁴⁶¹

r. Arista Records v. Myxer

In Arista Records LLC v. Myxer Inc.,³⁴⁶² the defendant Myxer operated a website that enabled registered users to upload recorded music to the site and then, through the use of Myxer's software, to transcode the music into a format to create and download ringtones. Users could make ringtones they had created available for download to other users. In addition to uploading and downloading ringtones, Myxer users could play portions of any of the sound recordings on Myxer's site. Users could also select a sound recording on Myxer's site and share it on certain third party websites such as Facebook. Finally, users could select a sound recording on Myxer's site, often a full-length recording, and "Customize It" (using editing tools provided by Myxer) by selecting a desired start and stop point for a ringtone. UMG Records, a competitor in the ringtone market, contended that, by storing copies of UMG's sound recordings on its servers, allowing users to download copies of its sound recordings to users' cell phones, and allowing users to preview its sound recordings on either the Myxer site or on users' cell phones, Myxer was a direct infringer of UMG's reproduction, distribution and digital public performance rights and a secondary infringer under theories of contributory and vicarious liability.³⁴⁶³

In response to UMG's motion for summary judgment, for the reasons set forth in Section II.A.4(q) above, the court found genuine issues of fact with respect UMG's claims of direct, contributory and vicarious liability. The court also found genuine issues of fact with respect to Myxer's assertion of the safe harbor under Section 512(c). As an initial matter, the court considered whether the alleged infringement resulting from both the uploading and downloading activities on Myxer's site could be considered to occur "by reason of the storage at the direction of a user" as required by Section 512(c). The parties agreed that the uploaded material was clearly covered by Section 512(c), but disputed whether the downloading activities of users were also covered. The court ruled that they were, because such downloading occurred "as a result of" the uploaded material which was stored on the system and therefore fit within the scope of Section 512(c)'s "by reason of the storage at the direction of a user of material."³⁴⁶⁴

The court then turned to whether Myxer had satisfied the threshold requirements of the Section 512(c) safe harbor relating to a repeat infringer policy:

-- The court found that Myxer had provided evidence of the existence of a repeat infringer policy. Myxer's "Abuse" page on its site had always stated that Myxer would terminate access for repeat infringers, and when a user registered with the site, the user was required to agree to a statement that he or she understood that uploading material in violation of the site's

³⁴⁶¹ Id. at 52 (citing Viacom Int'l v. YouTube, Inc., 676 F.3d 19, 30-41 (2d Cir.2012)).

³⁴⁶² 2011 U.S. Dist. LEXIS 109668 (C.D. Cal. Apr. 1, 2011).

³⁴⁶³ Id. at *2, *15-18.

³⁴⁶⁴ Id. at *55-56.

Terms of Use, which prohibited using the site to upload or transmit any infringing material, would result in the canceling of the user's account. UMG acknowledged that Myxer had a repeat infringer policy as to users who uploaded, but argued that it had no policy as to users who downloaded infringing material, because only users who wanted to upload were required to register and agree to the Terms of User, whereas there was no registration requirement for users who only downloaded material. Myxer argued that the DMCA does not require it to have a system in place to prevent users from downloading from its site because requiring registration for uploading should sufficiently prevent and stop infringing activity.³⁴⁶⁵ The court concluded the following:

To the extent that Myxer contends that it qualifies for the safe harbor because, as a matter of law, it has no obligation to establish a repeat infringer policy for users who download copyrighted material goes too far. That argument is based on the proposition that users do not have to register to access the site and implies that Myxer can avoid liability simply by declining to register users. But if internet service providers can so easily avoid liability for infringement, the constraints imposed by § 512(i)(A)'s requirements cease to have any meaning. ... [But] to the extent that Myxer's repeat infringer policy as to uploading meaningfully prevents users from accessing infringing material and can be reasonably adopted and implemented, Myxer's repeat infringer policy complies with the purpose of the DMCA and § 512(i). ... Consequently, because users are necessarily limited to downloading already uploaded material and Myxer's repeat infringer policy as to users who upload infringing material is appropriate and reasonable, a strong argument can be made that a repeat infringer policy as to users who download would be redundant. Stated another way, to the extent that adopting a repeat infringer policy as to users who download is not feasible, the Court is compelled to construe any such policy beyond the realm of appropriate and reasonable.³⁴⁶⁶

The court therefore concluded that Myxer had sufficiently demonstrated the existence of a repeat infringer policy, and whether that policy was adequate to meet the requirements of the DMCA was an issue that must be resolved at trial.³⁴⁶⁷

-- The court concluded that, because Myxer's Terms of Use indicated that Myxer reserved the right to terminate repeat infringers' ability to upload, Myxer had raised a genuine issue of material fact as to whether it reasonably communicated a repeat infringer policy to users.³⁴⁶⁸

-- The court concluded that Myxer had also raised a genuine issue of material fact as to whether it reasonably implemented its repeat infringer policy. Myxer's copyright compliance

³⁴⁶⁵ Id. at *57-60.

³⁴⁶⁶ Id. at *60-61.

³⁴⁶⁷ Id. at *63.

³⁴⁶⁸ Id. at *66-67.

officer and designated DMCA officer stated that she processed DMCA notices immediately and disabled infringing material usually within one business day of the notice and also disabled access to material and terminated users in response to informal notices as well as DMCA-compliant ones. UMG argued that Myxer's implementation of the policy was inadequate because, even if a user was terminated, that user could immediately re-register with a different user name and resume infringing. The court rejected this argument, noting that UMG had cited no controlling authority indicating that such a set of circumstances would render a policy insufficient under the DMCA. Moreover, even if UMG had provided evidence of users re-registering after their accounts had been terminated, that would not necessarily evidence a failed implementation of the policy.³⁴⁶⁹

The court then turned to the knowledge prong of the Section 512(c) safe harbor. Looking first at the issue of actual knowledge, the court noted as an initial matter that general awareness of infringement on the site, without more, is not enough to preclude application of Section 512(c). The existence of some licenses between Myxer and third parties with respect to some sound recordings used on the site diminished the plaintiff's argument that Myxer had actual knowledge of infringement because any awareness of copyrighted material may have related to licensed material only. Nor did Myxer have an obligation to actively seek out actual knowledge of infringing material by searching its system. Accordingly, because the burden is on the copyright holder to give notice of allegedly infringing material and Myxer provided evidence that notice from UMG was insufficient (coming only in the form of the complaint filed against Myxer) and it did not have actual knowledge of the alleged infringement, UMG was not entitled to summary judgment to the extent it sought to find that Myxer had actual knowledge.³⁴⁷⁰

Turning next to the issue of red flag knowledge, the court rejected UMG's argument that Myxer's awareness of "Most Popular" downloads, "Recent Downloads", and "Just Shared" files – which UMG argued must undoubtedly be copyrighted – did not, as a matter of law, establish knowledge of a red flag. The court also rejected UMG's argument that Myxer should have implemented the Audible Magic fingerprinting system and that failure to do so indicated the existence of willful blindness to widespread infringement because implementation would have confirmed that infringement was occurring. But the court noted that it was not clear whether the DMCA imposes an obligation on a service provider to implement filtering technology at all, because the DMCA does not place the burden of ferreting out infringement on the service provider. Although the use or non-use of filtering tools was not irrelevant, taken alone, the failure to develop or use a filter would be insufficient to support liability and must be considered in context with other evidence to determine existence of an unlawful objective on the part of the

³⁴⁶⁹ *Id.* at *69-71. Myxer also submitted evidence that it had a "Take Down, Stay Down" policy that used Audible Magic's filtering technology to block future uploads of works identified in DMCA notices from being uploaded to Myxer's site. The "Stay Down" list included more items than DMCA notice received because Myxer removed any existing items from the same users/titles it could locate and added those works to its "Stay Down" list. *Id.* at *23-24.

³⁴⁷⁰ *Id.* at *79-84.

service provider. Accordingly, UMG was not entitled to summary judgment to the extent its motion was based on red flag knowledge.³⁴⁷¹

The court found material issues of fact with respect to whether Myxer had carried out expeditious removal of infringing works after receiving notice. UMG claimed that Myxer had never terminated any user its policy of repeat infringers and that, even if it did so, the user could immediately re-register with a different user name and continue infringing. Myxer, on the other hand, presented evidence that it responded to DMCA notices, removed infringing material within one business day of receiving notices, had disabled more than 23,000 items in response to DMCA notices or for suspected infringement, and had terminated at least 2,371 individual user accounts pursuant to its policy that required termination of accounts that had been subject to two DMCA notifications.³⁴⁷²

With respect to the financial benefit prong of Section 512(c), the court noted that the central question in this case was whether the infringing activity constituted a draw for users to the site, not just an added benefit. The court noted that the relevant inquiry was whether there was a causal relationship between the infringing activity and any financial benefit Myxer received, and noted that the record supported the conclusion that Myxer undoubtedly received some financial benefit from the infringing activity. However, to the extent that infringing material represented only 1% of total uploaded material on the site, it remained unclear to what degree UMG's works served as a draw. The court concluded that, without more, it could not on a motion for summary judgment resolve the issue in favor of UMG and against Myxer.³⁴⁷³

Finally, with respect to the right and ability to control prong, the court agreed with numerous other decisions that the mere ability of a service provider to remove or block access to materials posted on its site or stored in its system is insufficient to satisfy the right and ability to control requirement. UMG argued that Myxer could control infringement because virtually all of the MP3 files uploaded to its site by users were embedded with metadata containing the name of the song, the recording artists, and, sometimes, the copyright owner, which Myxer could use to filter out works for which it possessed no rights, but it had chosen not to do so. The court rejected this argument, noting that the DMCA does not require service providers to deal with infringers in a particular way, such as by implementing filtering of the sort identified by UMG. Moreover, the court noted that the allegedly infringing works were not uploaded by Myxer, Myxer did not select or preview them, and the processing of uploads into downloadable format was entirely automated. Accordingly, because the evidence was in conflict regarding whether and to what extent Myxer had the right and ability to control infringing activity, UMG's motion for summary judgment with respect to the safe harbor was denied.³⁴⁷⁴

³⁴⁷¹ Id. at *86-89.

³⁴⁷² Id. at *25,

³⁴⁷³ Id. at *97-98.

³⁴⁷⁴ Id. at *107-09.

s. Flava Works v. Gunter

The facts of this case are set forth in Section III.C.1(b). In granting the plaintiff's motion for a preliminary injunction, the court ruled that the defendants were not entitled to the Section 512(c) safe harbor because they had not adopted and reasonably implemented a repeat infringer policy. The owner/operator of the myVidster web site had adopted a definition of "infringer" to mean a user who posted a link to content that was not otherwise publicly available on another web site – i.e., content that was hosted on a password-protected or private web site. The court ruled that this definition did not encompass the law of copyright's definition of "infringer," and therefore any repeat infringer policy based on such a definition could not be adequate. In addition, although the owner/operator removed videos listed in DMCA notices, he did not go any further to terminate users who were the subject of repeat infringement notices.³⁴⁷⁵

The Seventh Circuit reversed on appeal, finding that the safe harbor was irrelevant because the defendants were not liable for copyright infringement, and vacated the preliminary injunction, for the reasons discussed in Section III.C.2(m) above.³⁴⁷⁶

t. Capitol Records v. MP3tunes

The District Court's 2011 Decision

The case of Capitol Records, Inc. v. MP3tunes, LLC³⁴⁷⁷ tested whether the operator of a music "locker" service is liable for infringing music files stored in its users' lockers. The defendant MP3tunes operated a storage service that allowed users to store music files in personal online storage "lockers." Songs uploaded to a user's locker could be played and downloaded through any Internet-enabled device. MP3tunes offered free lockers with limited storage space and premium lockers with expanded storage for a subscription fee. The defendant also offered another feature of its web site called "Webload" that allowed a user to enter the web address of a music file stored on a third-party Internet server and transfer the file to the user's locker. MP3tunes used the standard Content-Addressable Storage system to store music files on its servers. Based on the sequence of data bits in a particular music file, the algorithm created a hash tag as an identification number. If different users uploaded the same song containing identical blocks of data to MP3tunes' servers, those blocks were assigned the same hash tag and typically saved only once. If a user played or downloaded a song from a locker, the

³⁴⁷⁵ Flava Works, Inc. v. Gunter, 2011 U.S. Dist. LEXIS 82955 at *30-32 (N.D. Ill. July 27, 2011), rev'd, 689 F.3d 754 (7th Cir. 2012).

³⁴⁷⁶ Flava Works, Inc. v. Gunter, 689 F.3d 754 (7th Cir. 2012).

³⁴⁷⁷ 821 F. Supp. 2d 627 (S.D.N.Y. 2011), rev'd in part and remanded sub nom. EMI Christian Music Group, Inc. v. MP3Tunes, LLC, 840 F.3d 69 (2d Cir. 2016).

storage system used the hash tags associated with the uploaded song to reconstruct the exact file the user originally uploaded to his or her locker.³⁴⁷⁸

MP3tunes also operated a second web site at www.sideload.com, which allowed users to search for free song files. Upon entering a keyword, the site would generate a list of potential matches by searching an index of web sites with free song files and cross-referencing the keywords with information associated with each song file. The index was maintained on MP3tunes' servers. After clicking on a search return, the user was taken to a page where he or she could play the song, follow a link to the third-party web site hosting the song, or download the song to another computer. If the user had a locker on MP3tunes.com, Sideload.com displayed a link that if clicked would "sideload" (download) the song from the third-party web site and save it to his or her locker. Importantly, MP3tunes kept track of the sources of songs in its users' lockers. Thus, MP3tunes could identify the third-party web sites from which users copied songs to their lockers. Sideload servers automatically generated lists of "Most Popular," "Featured," and "New" songs that users could browse.³⁴⁷⁹

Sideload.com also offered users free Sideload plug-in software. When a user of the plug-in came across a web site with a free song file, a button appeared on that site that would copy the song directly to the user's MP3tunes locker without visiting Sideload.com. When a user sideloaded a song from a third-party site, either through the Sideload plug-in or the Webload software, that third-party site was added to Sideload.com's index of searchable songs. Information associated with the song, such as artist, album, title, and track was automatically stored on a "Track Details" page, and the information became part of the searchable index. From then on, Sideload.com returned a potential match whenever any other user searched for that song on Sideload.com by entering keywords that matched the song file. When a downloadable song was removed from a third-party source, the Sideload feature became inoperable and users could no longer add the song to their lockers. However, users who sideloaded the song before it was removed from the third-party source could continue to access the song through their lockers.³⁴⁸⁰

The plaintiff record labels sought to hold MP3tunes liable for copies of infringing music files stored in its lockers and MP3tunes asserted the Section 512(c) safe harbor. One of the plaintiffs, EMI, had submitted a notice of infringement identifying 350 song titles and web addresses that allegedly infringed EMI's copyrights. It also provided a list of EMI artists and demanded that MP3tunes remove all of EMI's copyrighted works, even those not specifically identified with web addresses. MP3tunes removed links to the specific web addresses but did not remove infringing songs from its users' lockers. MP3tunes requested that EMI identify any

³⁴⁷⁸ *Id.* at 633-34.

³⁴⁷⁹ *Id.* at 634.

³⁴⁸⁰ *Id.* at 634-35.

other infringing links, which EMI declined to do, asserting that its representative list was sufficient to obligate MP3tunes to take down all other infringing material.³⁴⁸¹

EMI argued that MP3tunes had not satisfied the predicate conditions of Section 512(i) to qualify for the safe harbors because it had purposefully blinded itself to its users' infringement and failed to take any action against hundreds of users who sideloaded copies of songs identified in EMI's takedown notices. MP3tunes countered this argument by noting that it had terminated the accounts of 153 repeat infringers who violated copyrights by sharing the contents of their lockers with other users.³⁴⁸²

The court analyzed whether MP3tunes had satisfied the predicate conditions of Section 512(i) by drawing a distinction between "(1) users who know they lack authorization and nevertheless upload content to the internet for the world to experience or copy, and (2) users who download content for their personal use and are otherwise oblivious to the copyrights of others. The former are blatant infringers that internet service providers are obligated to ban from their websites. The latter, like MP3tunes users who sideload content to their lockers for personal use, do not know for certain whether the material they download violates the copyrights of others."³⁴⁸³ The court noted several cases (the Viacom, Io Group, and Corbis cases) requiring the termination of users who repeatedly upload copyrighted material to service providers' web sites, but absolving services providers from policing users who merely consume that content. The court also noted that, unlike in the Aimster case, MP3tunes had not purposefully blinded itself to its users' identities and activities. Rather, MP3tunes had tracked the source and web address of every sideloaded song in its users' lockers and could terminate the accounts of repeat infringers, which it had done in 153 instances. Finally, the court found that MP3 tunes had demonstrated it had a procedure for responding to DMCA takedown notices, and had used such procedure to remove all of the specific web addresses containing infringing files that EMI had identified.³⁴⁸⁴

The court rejected EMI's argument that MP3tunes had an obligation to terminate any user who added multiple links to Sideload.com that appeared on one or more takedown notices because they were automatic repeat infringers. The court noted that takedown notices themselves are not evidence of blatant infringement and users could not be certain that they had downloaded infringing content. Thus, MP3tunes' decision to refrain from termination of those user accounts was appropriate. Accordingly, the court ruled that MP3tunes had satisfied the predicate conditions of Section 512(i) for eligibility for the safe harbors.³⁴⁸⁵

³⁴⁸¹ Id. at 635.

³⁴⁸² Id. at 638.

³⁴⁸³ Id.

³⁴⁸⁴ Id. at 638-39.

³⁴⁸⁵ Id. at 639.

Turning to the specifics of the Section 512(c) safe harbor, the court first rejected EMI's argument, relying on Section 301(c) of the copyright statute,³⁴⁸⁶ that the safe harbors do not apply to songs recorded prior to Feb. 15, 1972. Although noting it was an issue of first impression, the court concluded that there is no conflict between Section 301 and the DMCA's safe harbors for infringement of pre-1972 recordings. The text of the DMCA limits immunity for the "infringement of copyrights" without drawing any distinction between federal and state law. Although Section 501(a) of the copyright statute makes anyone violating the rights established by Sections 106 through 122 an infringer, that section does not suggest that its list of acts constituting infringement is all inclusive. The court also noted that the DMCA was enacted to clarify copyright law for Internet service providers in order to foster fast and robust development of the Internet. Limiting the DMCA to recordings after 1972 would spawn legal uncertainty and subject otherwise innocent Internet service providers to liability for the acts of third parties. Accordingly, the court concluded that the DMCA's safe harbors, read in the light of their purpose, cover both state and federal copyright claims and apply to sound recordings fixed prior to Feb. 15, 1972.³⁴⁸⁷

Turning to the sufficiency of EMI's takedown notices, the court held that a notice merely stating "all songs" by a particular artist, or some other vague descriptor and nothing more, is inadequate to trigger a takedown obligation because it does not enable the service provider to locate the allegedly infringing material. Service providers must take down the specific infringing material identified in the notice but as a general matter are not required to search for and take down other material that may infringe the identified copyrighted works.³⁴⁸⁸ However, in this instance:

MP3tunes was obligated to remove specific works traceable to users' lockers. Because MP3tunes keeps track of the source and web address for each sideloaded song in each user's locker, EMI's notices gave sufficient information for MP3tunes to locate copies of infringing songs in user lockers. ... Where service providers such as MP3tunes allow users to search for copyrighted works posted to the internet and to store those works in private accounts, to qualify for DMCA protection, those service providers must (1) keep track of the source and web address of stored copyrighted material, and (2) take content

³⁴⁸⁶ Section 301(c) states, "With respect to sound recordings first fixed before February 15, 1972, any rights or remedies under the common law or statute of any State shall not be annulled or limited by this title until February 15, 2067."

³⁴⁸⁷ MP3tunes, 821 F. Supp. 2d at 640-42. In December 2011, the Copyright Office published a report concluding that the DMCA safe harbors do not apply to pre-1972 recordings. Federal Copyright Protection for Pre-1972 Sound Recordings (Dec. 2011), available at www.copyright.gov/docs/sound/pre-72-report.pdf. After publication of the report, the district court, in deciding a motion to certify an interlocutory appeal, noted that his decision with respect to applicability of the safe harbors to pre-1972 recordings "may involve a substantial ground for difference of opinion, particularly in light of the Copyright Office's determination that the DMCA safe harbors do not apply to pre-1972 recordings." Capitol Records, Inc. v. MP3tunes, LLC, 2012 U.S. Dist. LEXIS 8984 at *2 (S.D.N.Y. Jan. 9, 2012). The court, however, decided not to certify the issue for an interlocutory appeal. *Id.* at *10.

³⁴⁸⁸ MP3tunes, 821 F. Supp. 2d. at 642.

down when copyright owners identify the infringing sources in otherwise compliant notices.³⁴⁸⁹

The court held that there was no genuine dispute that MP3tunes did not qualify for safe harbor protection for songs stored in users' lockers that were sideloaded from the unauthorized web sites identified in takedown notices.³⁴⁹⁰

The court then turned to the question whether MP3tunes was disqualified from the Section 512(c) safe harbor by virtue of having actual or "red flag" knowledge of infringement with respect to which it failed to act. The court noted that the knowledge provisions are designed to deny safe harbor protection to Internet service providers operating or linking to pirate sites whose illegal purpose is obvious to a reasonable person, but general awareness of rampant infringement is not enough to disqualify a service provider of protection. EMI argued that MP3tunes had red flag knowledge in part because its executives sideloaded songs by popular artists from obviously infringing sites like rapidshare.com, fileden.com and filefactory.com. The court noted, however, that those sites do not use words like "pirate" or "bootleg" or other slang to indicate their illegal purpose and are not otherwise clearly infringing. Nor did the DMCA place the burden of investigation on MP3tunes to determine whether those sites were not authorized to distribute EMI's copyrighted works.³⁴⁹¹ Said the court, "Put another way, if investigation is required to determine whether material is infringing, then those facts and circumstances are not 'red flags.'"³⁴⁹² Because EMI itself regularly distributed work on the Internet for free, MP3tunes' executives and other Internet users had no way of knowing for sure whether free songs on the Internet were unauthorized. Accordingly, there was no genuine issue that MP3tunes did not have specific red flag knowledge with respect to any particular link on Sideload.com, other than the specific URLs noticed by the plaintiffs.³⁴⁹³

The court also ruled that MP3tunes was not disqualified from the safe harbors by virtue of having control and a financial benefit over the infringing activity. As to direct benefit, while Sideload.com could be used to draw users to MP3tunes.com and drive sales of pay lockers, it had noninfringing uses and MP3tunes did not promote infringement. Any link between infringing activity and a direct benefit to MP3tunes was attenuated because sideloaded songs were stored free of charge and infringing and noninfringing users of Sideload.com paid precisely the same or nothing at all for locker services. Nor did MP3tunes have control over its users' activity because its users alone chose the web sites they linked to Sideload.com and the songs they sideloaded

³⁴⁸⁹ *Id.* at 642-43. The court rejected MP3tunes' concern for liability if it removed material from its users' lockers: "MP3tunes exaggerates the potential liability of removing content from users' lockers. MP3tunes' Terms of Use clearly authorize it to block a user's access to material in lockers. And the DMCA provides MP3tunes with immunity and a procedure for dealing with claims from its users. 17 U.S.C. § 512(g)." *Id.* at 643.

³⁴⁹⁰ *Id.*

³⁴⁹¹ *Id.* at 643-44.

³⁴⁹² *Id.* at 644.

³⁴⁹³ *Id.* at 644-45.

and stored in their lockers.³⁴⁹⁴ In sum, the court concluded, “there is no genuine dispute that MP3tunes may claim safe harbor protection for EMI works stored on MP3tunes.com and EMI works linked to Sideload.com. However, MP3tunes does not qualify for safe harbor protection for songs sideloaded from links identified in [EMI’s] takedown notices which it failed to remove from user lockers.”³⁴⁹⁵

The court went on to hold that MP3tunes could have contributory liability for the infringing material that remained in users’ lockers and for which it had received notices of infringement. The takedown notices from EMI were sufficient to establish no genuine dispute that MP3tunes had actual knowledge its users had stored and continued to have access to infringing copies of the plaintiffs’ works. And MP3tunes had made a material contribution to the infringing activity because its servers were the sole instrumentality of its users’ infringement. The court rejected MP3tunes assertion of the Sony defense that its servers and lockers had substantial noninfringing uses because MP3tunes had a continuing relationship with its users. Here, MP3tunes continued to allow its users to store and access works in their lockers even though it knew they had unlawfully downloaded those works. The court therefore granted EMI’s motion for summary judgment on its claim for contributory infringement with respect to the songs listed on EMI’s takedown notices and which MP3tunes failed to remove from users’ lockers.³⁴⁹⁶

Finally, EMI argued, relying on the Cartoon Network case, that MP3tunes’ storage system violated its right to public performance because it employed a “master copy” to “rebroadcast” songs to users who uploaded different copies of the same song.³⁴⁹⁷ In a ruling that is a bit unclear in its factual rationale, the court rejected this argument:

EMI’s argument, however, mischaracterizes MP3tunes’ storage system. The record demonstrates that MP3tunes does not use a “master copy” to store or play back songs stored in its lockers. Instead, MP3tunes uses a standard data compression algorithm that eliminates redundant digital data. Importantly, the system preserves the exact digital copy of each song uploaded to MP3tunes.com. Thus, there is no “master copy” of any of EMI’s songs stored on MP3tunes’ computer servers.³⁴⁹⁸

Accordingly, MP3tunes was entitled to safe harbor protection against EMI’s public performance infringement claims.

³⁴⁹⁴ Id. at 645.

³⁴⁹⁵ Id. at 646.

³⁴⁹⁶ Id. at 648-49. The court also ruled that the founder was personally directly liable for songs he personally sideloaded from unauthorized sites. However, MP3tunes was not directly liable for his or other executives’ sideloading of songs because it was not clear they downloaded those songs during the course of their employment. Id. at 649.

³⁴⁹⁷ Id. at 649.

³⁴⁹⁸ Id. at 649-50.

In sum, the court granted EMI's motion for summary judgment on its claim of contributory infringement against MP3tunes for songs noticed in EMI's takedown notices and not removed from user lockers. The court granted MP3tunes' motion for summary judgment on its defense under the DMCA safe harbors with respect to all claims of infringement except with respect to songs noticed in EMI's takedown notices and not removed from user lockers.³⁴⁹⁹

The District Court's 2013 Decision Upon Reconsideration

Upon a motion for reconsideration based on the Second Circuit's rulings with respect to willful blindness in Viacom International, Inc. v. YouTube, Inc.,³⁵⁰⁰ the district court ruled that a jury could reasonably interpret several documents in the record as imposing a duty to make further inquiries into specific and identifiable instances of possible infringement. For example, an email received by MP3tunes in April 2007 gave a specific blog title and the email's author stated that everything he had posted there was in clear violation of the DMCA and requested that MP3tunes remove any MP3s that were linked to that site. Another email from November 2007 stated that if MP3tunes would search for a particular song title it would find five results, two of which pointed to a particular web site that blatantly acknowledged that it contained infringing MP3s. In a third email, an MP3tunes employee acknowledged that while it was not clear whether content from a particular user's site was all copyrighted material, it probably was. Accordingly, the court vacated that portion of its October 2011 order granting summary judgment to the defendants on the issue of contributor infringement liability for those songs not subject to DMCA-compliant takedown notices, concluding that factual issues precluded summary judgment.³⁵⁰¹

The court also reconsidered its grant of summary judgment with respect to red flag knowledge in view of the fact that after Viacom, something less than a formal takedown notice may establish red flag knowledge. The court concluded that the issue of the defendants' red flag knowledge could not be resolved on summary judgment.³⁵⁰²

In its October 2011 order, the court had dismissed EMI's standalone claim for inducement as duplicative of its contributory copyright infringement claim. EMI asked for reconsideration of that ruling as well, arguing that footnote 5 in the Viacom decision had cited the Supreme Court's Grokster decision for the observation that secondary copyright infringement includes contributory, vicarious and inducement liability. EMI therefore asked the court to revive its inducement claims as a separate cause of action. The court took no position on whether inducement is a separate cause of action because in this case the evidence of record

³⁴⁹⁹ Id. at 650-51.

³⁵⁰⁰ 676 F.3d 19 (2d Cir.2012).

³⁵⁰¹ Capitol Records, Inc. v. MP3tunes, LLC, 2013 U.S. Dist. LEXIS 68793 at *10, *14-16 (S.D.N.Y. May 14, 2013), rev'd in part and remanded sub nom. EMI Christian Music Group, Inc. v. MP3Tunes, LLC, 840 F.3d 69 (2d Cir. 2016).

³⁵⁰² Id. at *18.

was not sufficient to meet the high degree of proof required for an inducement claim.³⁵⁰³ The court, however, observed the following in dicta:

This Court is aware of no authority for the proposition that the DMCA safe harbor is per se unavailable in an inducement claim, or that evidence of inducement would obviate the requirement to prove actual or red flag knowledge of infringement. Rather than introducing a categorical bar to the safe harbor, the case law indicates only that inducement conduct may be relevant to establish an exception to safe harbor protection, such as actual or apparent knowledge of infringement. ... This is not a remarkable observation given that the DMCA safe harbor exceptions are aimed at bad faith infringers.³⁵⁰⁴

Lastly, MP3tunes requested reconsideration of the court's ruling with respect to its supply of cover art to its locker users. Pursuant to a licensing agreement with Amazon, MP3tunes offered users a "Lockersync" function that allowed users to retrieve and display the corresponding cover art from Amazon while playing a song in their MP3tunes lockers. If cover art was not part of a music file or stored on a user's computer, Lockersync retrieved the cover art from Amazon and displayed a link to that web site. EMI maintained that MP3tunes directly infringed its copyrights in the cover art. In its October 2011 order, the district court had found questions of fact precluded summary judgment because of contradictory proof on the issues of MP3tunes' use and storage of cover art and the direction of traffic to Amazon.³⁵⁰⁵

MP3tunes contended that Viacom precluded copyright infringement liability for the cover art because it was protected by the Section 512(c) safe harbor. In Viacom, the Second Circuit found that YouTube's "related videos" function, by which a YouTube computer algorithm identified and displayed thumbnails of clips that were related to the video selected by the user, was protected by the Section 512(c) safe harbor, which the Second Circuit ruled extends to software functions performed for the purpose of facilitating access to user stored material. MP3tunes' cover art function used an algorithm that retrieved, copied, stored, and displayed cover art from Amazon related to those songs a user chose to sideload. The district court noted that, while MP3tunes' cover art algorithm retrieved and copied cover art solely in response to a user's song selection, the cover art itself was provided by Amazon, not other MP3tunes users. As such, the cover art was not stored at the direction of a user, but rather presented to users by Mp3tunes as part of an automated marketing ploy. Thus, the primary purpose of the cover art algorithm was not narrowly tailored to facilitate access to user stored material, but rather to prompt users to go to a separate web site entirely for the purpose of purchasing music. The

³⁵⁰³ Id. at *19-23.

³⁵⁰⁴ Id. at *21-22.

³⁵⁰⁵ Id. at *23-24.

court therefore declined to rule that MP3tunes' cover art algorithm was shielded by the Section 512(c) safe harbor, and EMI's cover art infringement claim must proceed to trial.³⁵⁰⁶

The Jury Verdict and the District Court's Opinion on Robertson's Post-Trial Motions

In March of 2014, a jury found MP3tunes directly liable for infringement of the plaintiff's reproduction and public display rights in cover art and for unfair competition with respect to pre-1972 sound recordings. Concluding that MP3tunes acted with both red flag knowledge and willful blindness, the jurors found MP3tunes secondarily liable for infringements by MP3tunes' users, third party websites, and MP3tunes executives. Finally, the jury did not find MP3tunes secondarily liable for violating the plaintiffs' distribution rights. While the jury did not hold founder Michael Robertson contributorily liable for MP3tunes' failure to remove certain works from lockers in response to takedown notices, it imposed secondary liability on Robertson for every other claim on which it held MP3tunes liable. During the damages phase, the jury found MP3tunes and Robertson acted willfully as to all infringing acts except for MP3tunes' failure to remove works from lockers. The jury awarded the plaintiffs \$48,061,073 in damages.³⁵⁰⁷

Robertson then moved for judgment as a matter of law, or alternatively a new trial, and for remittitur. The court mostly denied Robertson's motions, granting them only to the following extent:

-- It granted JMOL as to Robertson's liability for secondary infringement for tracks sideloaded by users from domains that were listed ten or more times in takedown notices. The court ruled that red flag knowledge requires awareness of facts that would have made *specific* instances of infringement objectively obvious to a reasonable person. Knowledge that a high percentage of content on a domain is infringing does not establish actual or red flag knowledge of particular instances of infringement. It was therefore impermissible to impute red flag knowledge or willful blindness to MP3tunes or Robertson based on such domains because doing so would impose an obligation to affirmatively monitor content, in contravention of Section 512(m)'s clear instruction that no such obligation exists.³⁵⁰⁸

-- Similarly, the court granted JMOL as to Robertson's secondary liability for infringement for all tracks sideloaded pre-2007, which the plaintiffs argued the defendants should have known were infringing since the major record labels offered no MP3s for sale until 2007. The court ruled that knowledge that a high percentage of a type of content is infringing is insufficient to create red flag knowledge. And given that under the DMCA, service providers are under no obligation to conduct routine searches and eliminate material likely to be infringing, neither

³⁵⁰⁶ Id. at *24-27.

³⁵⁰⁷ Capitol Records, Inc. v. MP3tunes, LLC, 48 F. Supp. 3d 703, 711 (S.D.N.Y. 2014), rev'd in part and remanded sub nom. EMI Christian Music Group, Inc. v. MP3Tunes, LLC, 840 F.3d 69 (2d Cir. 2016).

³⁵⁰⁸ Id. at 716.

MP3tunes nor Robertson could be held liable for failing to routinely search its servers for major-label MP3s released before January 2007.³⁵⁰⁹

-- The court granted JMOL as to Robertson's secondary liability for users' sideloading of tracks by The Beatles, except as to the song "Strawberry Fields Forever" (because a user had sent MP3tunes an email indicating that song was available on Sideload.com) and those Beatles songs sideloaded by MP3tunes executives themselves. Apart from those specific instances, the record was bereft of any other evidence supporting the jury's finding of red flag knowledge and willful blindness as to specific works by The Beatles.³⁵¹⁰

-- The court granted JMOL as to Robertson's liability for public display of cover art. Each time any user uploaded a track, MP3tunes' software automatically searched for and retrieved cover art, regardless of whether other users had that cover art in their lockers. Only one user was capable of receiving each copy. Because there was no master copy of the cover art, neither MP3tunes nor Robertson could be held directly liable for a public display of cover art.³⁵¹¹

-- The court granted JMOL to Robertson with respect to certain statutory damages pertaining to cover art. Specifically, although the plaintiffs had submitted general evidence that cover art was available to digital service providers at the same time as the songs, and that cover art was generally commercially exploited by publishers through the use of merchandise, there was no evidence that each and every cover art work was made available separately. And there was no way to determine, based on the trial record, which cover art was or was not available separately. Had the plaintiffs proved that the cover art was available separately, then they could recover for infringement of such art separate from the recovery of the sound recording. But they did not. Accordingly, the court ruled that recovery was available only for cover art for which the plaintiffs had not recovered on a sound recording.³⁵¹²

-- Finally, the court granted Robertson's motion for a new trial on the punitive damage award (based on the plaintiffs' unfair competition and common law copyright claims for any pre-1972 sound recordings in suit) unless the plaintiffs elected to remit the jury's punitive damage award from \$7.5 million to \$750,000. The court found that the \$7.5 million punitive damage award violated due process, largely based on the fact that the plaintiffs had sought, and the jury awarded, only nominal actual damages of \$1 per work. The court noted that the effect of its rulings on willful blindness and red flag knowledge had reduced the nominal damages award to only \$40 (Robertson and MP3tunes remained liable for 40 pre-1972 works – "Strawberry Fields Forever," 16 works sideloaded by executives, and 23 works from source domains seen by

³⁵⁰⁹ Id. at 716-17.

³⁵¹⁰ Id. at 717-18.

³⁵¹¹ Id. at 720-21.

³⁵¹² Id. at 722-23.

executives that were obviously infringing). Given this tiny amount of actual damages, a punitive award of \$7.5 million was grossly excessive.³⁵¹³

The Second Circuit's 2016 Decision

The plaintiffs appealed several issues relating to MP3tunes' liability and damages, and Robertson cross-appealed several issues as well, some relating to the liability of MP3tunes and some relating to his own personal liability. The Second Circuit (1) vacated the district court's grant of partial summary judgment to the defendants based on its conclusion that MP3tunes qualified for safe harbor protection under the DMCA because the district court applied too narrow a definition of "repeat infringer," (2) reversed the district court's grant of summary judgment as a matter of law to the defendants on claims that MP3tunes permitted infringement of the plaintiffs' copyrights in pre-2007 MP3s and Beatles songs because there was sufficient evidence to allow a reasonable jury to conclude that MP3tunes had red flag knowledge of, or was willfully blind to, infringing activity involving those categories of protected material, (3) remanded for further proceedings related to claims arising out of the district court's grant of partial summary judgment, and (4) affirmed the judgment in all other respects.³⁵¹⁴

The court turned first to the plaintiffs' appeal. First, the plaintiffs challenged the district court's ruling that MP3tunes reasonably implemented a repeat infringer policy and was eligible for DMCA safe harbor protection. The court noted that to resolve the plaintiffs' challenges, it must answer two related questions: whether certain MP3 tunes users qualified as "repeat infringers," and if so, whether MP3tunes reasonably implemented a policy directed at them. For purposes of Section 512(i)(1)(A), the district court had defined a "repeat infringer" as a user who *uploaded* infringing content to the internet knowing that the conduct infringed another's copyright, but that a user who *downloaded* songs from third-party sites for their personal enjoyment could not be a repeat infringer. The district court thus concluded that only users who upload infringing content are blatant infringers that service providers are obligated to ban from their web sites.³⁵¹⁵

The Second Circuit faulted the district court on its knowledge requirement and its conclusion that only uploaders can be repeat infringers. The Second Circuit ruled that the district court was wrong to incorporate a knowledge requirement into the definition of "repeat infringer," because copyright is a strict liability offense that does not require unlawful intent or culpability. Thus, in the context of this case, all it took for a user to be a "repeat infringer" was to repeatedly sideload copyrighted material for personal use. Moreover, given that the DMCA imposes certain requirements on service providers in exchange for limitations on liability, it would make little sense to link that limitation on liability to the knowledge of users. And Section 512(m) of the DMCA explicitly relieves service providers from having to affirmatively monitor their users for infringement – something that would likely be required should MP3tunes have to

³⁵¹³ *Id.* at 727-33.

³⁵¹⁴ *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 840 F.3d 69, 75-76 (2d Cir. 2016).

³⁵¹⁵ *Id.* at 78-79.

ascertain its users' knowledge. In a footnote, the court noted that the Nimmer treatise links the term "repeat infringer" more directly to the knowledge of the *service provider* rather than user. Specifically, the treatise defines an "infringer" as either a party who has been adjudicated to have committed copyright infringement or a party about whom the service provider has actual knowledge that the person engaged in infringement. The treatise cautions that a service provider must have done more than just receive a copyright holder's takedown notices in order to be charged with knowledge of infringement. The Second Circuit noted that in view of the facts of this case, it need not decide whether takedown notices suffice on their own to prove that the provider was aware of infringement. Finally, the court noted that no other circuit court had adopted a definition of "repeat infringer" that would include only those who willfully infringe copyrights.³⁵¹⁶

Under a correct definition of "repeat infringer," there was sufficient disputed evidence relating to MP3tune's policy regarding infringers to conclude that summary judgment was inappropriate. MP3tunes proffered evidence that it terminated 153 users who shared locker passwords. In response, however, the plaintiffs demonstrated that MP3tunes did not even try to connect known infringing activity of which it became aware through takedown notices to users who repeatedly sideloaded files and created links to that infringing content in the sideload.com index. And the plaintiffs presented evidence that MP3tunes executives were encouraged to and did personally sideload songs from blatantly infringing web sites. The same executives made the songs available to sideload.com users, and there was evidence that MP3tunes was capable of cataloging the sideloads of each MP3 user. A jury could therefore reasonably infer that MP3tunes actually knew of specific repeat infringers and failed to take action. Alternatively, a reasonable jury could have determined that MP3tunes consciously avoided knowing about specific repeat infringers using its services, even though the infringement was rampant and obvious, if at trial the plaintiffs could demonstrate that MP3tunes's failure to track users who created links to infringing content identified on takedown notices or who copied files from those links evidenced its willful blindness to the repeat infringing activity of its users.³⁵¹⁷

The court emphasized that its rulings were not inconsistent with the provisions of Section 512(m) that the safe harbor cannot be conditioned on a service provider monitoring its service or affirmatively seeking facts indicating infringing activity. Based on available evidence, a reasonable jury could have concluded that it was reasonable for MP3tunes to track users who repeatedly created links to infringing content in the sideload.com index or who copied files from those links. After all, MP3tunes had already tracked and removed 153 users who allowed others to access their lockers and copy music files without authorization. By comparison, requiring MP3tunes to extend that policy to users who sideloaded infringing content might not be an unreasonably burdensome request. And doing so would not require MP3tunes to monitor or affirmatively seek facts about infringing activity in a manner inconsistent with Section 512(m) because it already had adequate information at its disposal in the form of takedown notices provided by a plaintiff as to which links were allegedly infringing. MP3tunes would simply have

³⁵¹⁶ *Id.* at 79-80 & n.5.

³⁵¹⁷ *Id.* at 80.

had to make use of information already within its possession and connect that information to known users. While the defendants could yet make the case at trial that it was unreasonable under the circumstances to ask MP3tunes to identify users who repeatedly infringed plaintiffs' copyrights by sideloading music files, no evidence available at the summary judgment stage compelled that conclusion as a matter of law.³⁵¹⁸

The court then turned to the district court's granting of judgment as a matter of law in favor of the defendants with respect to MP3s from major labels issued before 2007 and all songs by the Beatles. The Second Circuit concluded that the facts, viewed in the light most favorable to plaintiffs, showed that MP3tunes and Robertson knew that major music labels generally had not authorized their music to be distributed in the format most widely available on sideload.com, let alone authorized it to be shared on the Internet. And in particular, Robertson knew that major record labels had not offered songs in MP3 format until 2007. The district court ruled, however, that barring MP3tunes from the safe harbor would require it to actively conduct routine searches and eliminate material likely to be infringing. The Second Circuit disagreed with this assessment. First, the jury was instructed, and the court presumed it understood, that MP3tunes had no continuing, affirmative duty to monitor its servers for infringement. The jury could comply with that instruction and still find that MP3tunes was required to disable access to pre-2007 songs. There was evidence at trial that MP3tunes could disable such access – an expert had testified that searching through libraries of MP3 songs was a common function of MP3tunes's business. The jury was therefore permitted to conclude that a time-limited, targeted duty – even if encompassing a large number of songs – did not give rise to an amorphous duty to monitor in contravention of Section 512(m) of the DMCA.³⁵¹⁹

The same was true of the Beatles songs. The jury heard evidence that Robertson knew there had been no legal online distribution of Beatles tracks before 2010, other than one track used within a video game. And a 2009 email showed that Robertson was aware of the plaintiffs' position that the Beatles had never authorized their songs to be available digitally. MP3tunes had been made aware through user emails that Beatles songs were on sideload.com's index. The jury could therefore have reasonably concluded that MP3tunes had red flag knowledge of, or was willfully blind to, the infringing nature of the Beatles tracks on its servers and failed to act to remove them.³⁵²⁰

The jury could also reasonably have found that MP3tunes conceived of and was designed to facilitate infringement based in part on evidence presented at trial that MP3tunes actively encouraged infringement and that Robertson and MP3tunes executives personally used sideload.com to download infringing material. In particular, the jury could reasonably have understood Robertson to have admitted on cross examination that sideload.com was premised on the notion that everything that was on the Internet that was not locked down could be sideloaded into the site. The Second Circuit therefore reversed the district court's ruling

³⁵¹⁸ *Id.* at 80-81.

³⁵¹⁹ *Id.* at 82-83.

³⁵²⁰ *Id.* at 83.

vacating the jury verdict with respect to red flag knowledge and willful blindness for pre-2007 MP3s and Beatles songs.³⁵²¹

The court affirmed the district court's ruling that the plaintiffs could recover only one statutory damages award for a musical composition and its corresponding sound recording, even where the composition and the recording were owned by separate plaintiffs. The court found that a plain reading of the copyright statute's text supported such conclusion, because sound recordings are defined in Section 101 as a species of derivative work of the underlying musical composition and thus both fall within the one-work-one-award rule for statutory damages. The court also found support for its conclusion in the House Report and Senate Report accompanying the 1976 Copyright Act, and therefore affirmed the district court's statutory damages award.³⁵²²

The court then turned to Robertson's cross appeal. Robertson first argued that the district court erred in upholding the jury's verdict of red flag knowledge and willful blindness with respect to songs sideloaded from personal file storage sites and student-run college web pages with what were alleged to be obviously infringing URLs. The court rejected this argument. The trial evidence supported the plaintiffs' argument that Robertson and MP3tunes executives knew that personal file storage sites and college student web pages were distributing infringing files. There was also evidence that Robertson himself sideloaded from personal web sites, and that other MP3tunes executives regularly sideloaded from those sites. The jury could therefore conclude that MP3tunes knew that songs from sites with personal file storage or college URLs were available on sideload.com and that those sites were obviously infringing, yet failed to act on that information. The court therefore affirmed the district court's order denying judgment as a matter of law with respect to this category of songs.³⁵²³

Robertson next challenged the jury's finding that MP3tunes was liable for directly and willfully infringing all 296 works of cover art associated with the plaintiffs' songs and albums. Although the district court vacated the verdict as to some of the cover art, Robertson argued that the entire verdict relating to cover art infringement should have been vacated. He argued that MP3tunes could not have engaged in a volitional act required for direct liability with respect to the cover art infringement because the retrieval of that art was not directed by MP3tunes but rather obtained from Amazon.com at the direction of the user when the user selected a song. The court found that the record contradicted Robertson on the point. MP3tunes's employees testified that the company's LockerSync system was designed to retrieve the album art whenever a user uploaded the song. The system thus retrieved a copyrighted item that the user did not request, frequently without the user's knowledge of the copyrighted nature of the item. That constituted sufficient evidence that copying of the cover art was directed by MP3tunes, not users. And a jury could reasonably have inferred that each of the 296 images had been

³⁵²¹ Id.

³⁵²² Id. at 84-85.

³⁵²³ Id. at 85.

downloaded from Amazon.com at least once because the evidence presented at trial showed that each image was actually downloaded several times.³⁵²⁴

The court also affirmed the jury's finding of liability on the part of three MP3tunes executives other than Robertson on a theory of respondeat superior. The court noted an email from one of the executives asserting that MP3tunes employees would seed the sideload.com index with higher quality tracks. An MP3tunes employee testified that she and other employees specifically sought out web sites to locate files and sideload them into the Sideload index. And Robertson directed that same employee to provide other MP3tunes employees with a list of some sites featuring free MP3s for sideloading purposes.³⁵²⁵

The court next rejected Robertson's challenge that there was insufficient evidence to support the jury's finding that he was vicariously and contributorily liable for MP3tunes's infringements. With respect to vicarious liability, the district court had correctly instructed the jury that an obvious and direct financial interest may be established where infringing material acts as a draw to attract subscribers to a defendant's business, even if it is not the primary or even a significant draw. There was testimony by an employee that she and other employees used Sideload marketing efforts to get people to sign up for lockers and emphasized the availability of free music on sideload.com in trying to get users to purchase lockers. There was also evidence that Robertson, through a trust, was the near-exclusive funder of MP3tunes and thus had an obvious and direct financial interest in infringement that drew subscribers to MP3tunes.com.³⁵²⁶

The court also rejected Robertson's challenge to contributory liability. The court cited both the traditional test for contributory infringement – one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another – and the Supreme Court's formulation in Grokster that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties. Here, there was sufficient evidence to support a finding of contributory liability on Robertson's part. He personally encouraged his employees to sideload songs to add to the index. Many of those songs were from sites that contained pirated material. The entire point of sideloading to the index was to make more music available for user download, even though Robertson knew the music was generally not available for free in MP3 form. This, in turn, aided and abetted infringement by sideload.com users. The court also rejected Robertson's challenge to the jury instruction on contributory infringement, which used the phrase "substantially contributes," rather than "materially contributes" as used in the traditional formulation of the test for contributory liability. The court found the phrase used was not misleading and

³⁵²⁴ Id. at 86. The court also rejected Robertson's argument that the cover art copyrights were invalid because they have been improperly registered on a Form SR, also used for the corresponding sound recording. The court noted that a few years ago the Copyright Office issued a circular that expressly sanctioned the use of a Form SR to register both the recording and associated images. Id. at 8687.

³⁵²⁵ Id. at 87.

³⁵²⁶ Id. at 89.

adequately informed the jury of the law. Finally, the court rejected Robertson's argument that under the Sony case he could not be held secondarily liable as a matter of law because MP3tunes was capable of substantial noninfringing uses. The court noted that the Supreme Court had clarified in Grokster that where evidence goes beyond a product's characteristics or the knowledge that it may be put to infringing uses, and shows statements or actions directed to promoting infringement, Sony will not preclude liability. Here, the evidence showed that Robertson acted in a manner intended to promote infringement.³⁵²⁷

Finally, the Second Circuit rejected Robertson's challenge to the district court's award of multiple statutory damages for music singles as well as the albums on which they appear. The court noted that materials that are sold as part of a compilation, such as songs on an album, ordinarily are not deemed separate works for the purpose of statutory damages. But when a copyright holder or publisher issues material on an independent basis, the law permits a statutory damages award for each individual work. The inquiry is whether the copyright holder issued its works separately, or together as a unit. Here, the district court properly allowed separate statutory damages awards for songs that the plaintiffs issued as singles, even if those songs were also made available on albums.³⁵²⁸

u. Obodai v. Demand Media

In this case, the owner of a copyrighted work sought to hold the operator of a humor website, Cracked.com, liable for the posting of the plaintiff's work by a third party. The plaintiff did not notify the defendant that the third party had posted the plaintiff's work on Cracked.com before filing suit pro se. The court ruled that the defendant satisfied all the requirements for the Section 512(c) safe harbor. The defendant had adequately adopted and implemented a policy to terminate repeat infringers because Section 16 of its web site Terms and Conditions stated that Cracked could terminate any account or user for repeated infringement of intellectual property rights, including copyrights, and reserved the right to terminate an account or user for even one instance of infringement.³⁵²⁹

With respect to the requirement that the service provider accommodate and not interfere with standard technical measures, the court noted that an example of a party's failure to comply with standard technical measures may include conduct that advises or encourages users to conceal a work's copyrighted status. To the extent the plaintiff contested this issue, the plaintiff argued that Cracked distributed copyrighted texts and entered into some form of a distribution agreement. The court noted that, while probative of other relevant considerations,

³⁵²⁷ Id. at 89-90.

³⁵²⁸ Id. at 90-91.

³⁵²⁹ Obodai v. Demand Media, Inc., 2012 U.S. Dist. LEXIS 83109 at *3, *11 (S.D.N.Y. June 13, 2012), aff'd, 2013 U.S. App. LEXIS 10734 (2d Cir. May 29, 2013). The Terms and Conditions also listed the physical and email addresses of its copyright agent and set forth information that a copyright holder should forward if it believed that Cracked contained infringing content. Id. at *24.

these facts were not evidence of interference with standard technical measures under the DMCA.³⁵³⁰

Turning to the knowledge prong of Section 512(c), the court rejected the plaintiff's argument that Cracked had knowledge of the infringement based on keyword-targeted advertisements that appeared with the posts of the plaintiff's work by the third party. Even assuming arguendo that the ads were not automatically generated, the court ruled that the existence of such ads did not reflect awareness that the postings had infringed. The plaintiff also argued that Cracked used a software tool called Tynt to measure search engine traffic to specific pages. The court concluded that such a tool does not support an inference that the defendant was aware of infringement, and instead was relevant only as to the defendant's knowledge as to visitors' pageviews. Nor was the fact that the defendant had previously received a considerable number of DMCA takedown notices from copyright holders sufficient in view of the Second Circuit's ruling in Viacom that the defendant must have knowledge that the specific works in dispute were infringing, not merely knowledge or suspicion of broader infringement.³⁵³¹

The court found that the defendant had acted expeditiously to remove the infringing content by taking the content down after the plaintiff filed his complaint but before her served the defendant and had emailed the third party poster informing him of the infringement claim and stating that his profile on Cracked would be deleted. Finally, with respect to the issue of control, the court noted that the defendant's use of Tynt to monitor Cracked traffic reported only on site traffic volume and not the content of user postings, and therefore did not give the defendant control over infringing content. Accordingly, the court ruled that the defendant was entitled to the Section 512(c) safe harbor and entered judgment for the defendant.³⁵³²

On appeal, the Second Circuit affirmed in a three-paragraph per curium opinion, finding that Obodai's appeal was without merit "substantially for the reasons articulated by the district court in its well-reasoned summary judgment decision. In short, the district court correctly determined that Demand Media was eligible for the User Storage Safe Harbor under the Digital Millennium Copyright Act, 17 U.S.C. § 512, because the undisputed evidence established that Demand Media satisfied the requirements under § 512(c) and (i). The record does not support Obodai's assertion that Demand Media's use of the software tool 'Tynt' required the district court to reach a different result."³⁵³³

v. Agence France Presse v. Morel

³⁵³⁰ Id. at *13-14.

³⁵³¹ Id. at *16-18.

³⁵³² Id. at *19, *23 & *27.

³⁵³³ Obodai v. Cracked Entertainment Inc., 2013 U.S. App. LEXIS 10734

2-3 (2d Cir. May 29, 2013) (citation omitted).

In Agence France Presse v. Morel,³⁵³⁴ photographer Daniel Morel took photos of Port au Prince, Haiti, shortly after an earthquake devastated the city and posted the photos on TwitPic. There were no copyright notices on the images themselves, but Morel's TwitPic page included the attributions "Morel" and "by photomorel" next to the images. A few minutes after Morel posted his photos, Lisandro Suero copied the photos, posted them on his TwitPic page, and tweeted that he had "exclusive photographs of the catastrophe for credit and copyright." Suero did not attribute the photos to Morel. Agence France Presse (AFP) downloaded 13 of Morel's photos from Suero's TwitPic page (not knowing that Suero had copied them from Morel), placed them on an image forum and transmitted them to Getty, an image licensing company. Morel's photos were labeled with the credit line "AFP/Getty/Lisandro Suero," designating AFP and Getty as the licensing agents and Suero as photographer. Getty then licensed Morel's photos to numerous third party news agencies, including CBS and CNN. After learning that the photos did not belong to Suero, AFP issued a wire instruction to change the photographer credit from Suero to Morel. However, Getty continued to sell licenses to charities, relief organizations, and new outlets that variously credited AFP, Suero, or Morel as the photographer.³⁵³⁵

Shortly thereafter, Corbis, which acted as Morel's worldwide licensing agent emailed Getty asserting exclusive rights to Morel's photos. That afternoon, AFP issued a "kill" for 8 images listing Morel as photographer, but the "kill" did not include identical images credited to Suero or images never credited to Morel. Morel and Corbis alleged that AFP and Getty failed to observe or enforce the credit change instruction or the "kill," continued to license and sell Morel's photos, and derived a direct financial benefit as a result. AFP filed a suit, seeking a declaratory judgment that AFP did not infringe Morel's copyrights in certain photos. Morel counterclaimed against AFP and Getty, alleging that they had willfully infringed his copyrights and that AFP and Getty were secondarily liable for the infringement of others and had violated the CMI provisions of the DMCA.³⁵³⁶

After discovery, upon cross motions for summary judgment, the court determined that both AFP and Getty were direct infringers for the distribution of unauthorized copies of Morel's photos. The court rejected a defense asserted by AFP that it was licensed to distribute Morel's photos as a third party beneficiary of Twitter's Terms of Use (TOU) to which Morel was subject when he uploaded his photos onto TwitPics.³⁵³⁷ Specifically, the Twitter TOS provided: "By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed). ... You agree that this license includes the right for Twitter to make such Content available to other companies, organizations or individuals who partner with Twitter for the syndication, broadcast, distribution or publication of such

³⁵³⁴ 769 F. Supp. 2d 295 (S.D.N.Y. 2011).

³⁵³⁵ *Id.* at 298-300.

³⁵³⁶ *Id.* at 298, 300-301.

³⁵³⁷ Agence France Presse v. Morel, 934 F. Supp. 2d 547, 559-60, 564 & 583-84 (S.D.N.Y. 2013).

Content on other media and services, subject to our terms and conditions for such Content use.”³⁵³⁸ AFP argued that it was a third-party beneficiary of this license between Morel and Twitter, claiming in particular that the Twitter TOS intended to confer a benefit (in the form of a license) on Twitter’s other users, for the comments to the Twitter TOS noted that Twitter encouraged and permitted broad re-use of Content.³⁵³⁹

The court rejected this argument, noting that the test for determining whether a contract was made for the benefit of a third party is whether an intent to benefit a third party appears from the terms of the contract. A third party may be a third-party beneficiary to a contract if the terms of the contract necessarily require that the promisor conferred a benefit on that third party. The court found that the evidence did not reflect a clear intent to grant AFP a license to remove the photos at issue from Twitter and license them to third parties, not did it necessarily require such a license. The Twitter TOS spelled out expressly the entities to whom a license was granted – Twitter and its partners – and AFP did not contend that it was one of Twitter’s partners.³⁵⁴⁰ The court also noted that the explanatory comments to the TOS recited that “[y]ou retain your rights to any Content you submit, post or display” and “what’s your is yours – you own your content.”³⁵⁴¹ Those statements would have no meaning if the Twitter TOS allowed third parties to remove the content from Twitter and license it to others without the consent of the copyright holder.³⁵⁴²

Getty asserted the Section 512(c) safe harbor in its motion for summary judgment as a defense to any direct or secondary liability on its part. The court rejected Getty’s motion, finding a material dispute as to whether Getty qualified as a “service provider” for purposes of the safe harbor. Looking at the text of the definition of “service provider” in Section 512(k) in conjunction with dictionary definitions of “service,” the court concluded that a “service provider” is an entity that, in broad terms, facilitates, supports, or enables online access or the activities of users of the Internet, and an entity directly licensing copyrighted material online would not be a “service provider.” In the court’s view, licensing copyrighted material online more closely resembled the mere sale of goods (or intellectual property in this case) than facilitating users’ activities online. The court noted that every case of which it was aware in which a party was held to be a “service provider” under Section 512(k) reflected a fact pattern in which the party claiming the benefit of the DMCA safe harbor was doing something useful for other entities or

³⁵³⁸ Id. at 560.

³⁵³⁹ Id. at 560-61.

³⁵⁴⁰ Id. at 561-62.

³⁵⁴¹ Id. at 563.

³⁵⁴² Id. The court also rejected as a false dichotomy AFP’s argument that either its conduct must have been licensed or the uncountable number of daily re-tweets on Twitter and in the media where Twitter and TwitPic posts were copied, reprinted, quoted, and rebroadcast by third parties would all constitute copyright infringements. The court noted that, even assuming there may be *some* license to third parties granted by the Twitter TOS – for example, a license to re-tweet content posted on Twitter – that function of Twitter simply did not necessarily require the licensed urged by AFP or manifest an intent to grant such an unrestricted license. Id. at 564.

individuals, such as providing a file hosting or file sharing platform, rather than itself selling or licensing copyrighted material. The record before the court contained evidence from which a jury could infer that Getty did not, in fact, simply host AFP's images. Morel had presented evidence suggesting that the agreement between AFP and Getty granted Getty rights to itself license the images that AFP provided, and Getty employees were actively involved in the licensing of Morel's photos to at least certain charitable organizations. On such evidence, a jury could infer that Getty's role extended beyond merely providing a file hosting service to AFP, and that Getty itself acted as a licensor of the photos. The court therefore concluded that there was an issue of fact as to whether Getty qualified as a service provider for purposes of the Section 512(c) safe harbor.³⁵⁴³

Finally, the court concluded that there were disputes of fact precluding summary judgment on the issues of whether AFP and Getty were willful infringers and liable as secondary infringers,³⁵⁴⁴ but went on to make rulings with respect to a dispute as to how the statutory damages provision of Section 504(c) would be applied to the facts of the case. Specifically, the parties disputed the proper application of Section 504(c)(1) to cases involving an alleged infringer who, through principles of secondary liability, may be found jointly liable with a number of alleged downstream direct infringers, none of whom are jointly liable with the other alleged downstream infringers. Morel argued that Getty and AFP were liable for not just a single statutory damages award for each work infringed, but rather a separate award of statutory damages for each distinct subscriber with whom they were jointly and severally liable.³⁵⁴⁵

The court rejected Morel's argument, noting that it would effectively bypass the limit of a single statutory award for "all infringements" of a work because it would hold Getty or AFP liable for multiple infringements of a single work. That conclusion was further supported by Section 504(c)(1)'s provision that a group of defendants who are all jointly and severally liable with each other are also to be liable for only a single statutory damages award, suggesting that a copyright holder should not be allowed to multiply damages against an infringer based on the infringing activity of jointly liable third parties. The court found that Congress' intent appears to have been to restrict statutory damages to a single award per work, per infringer, and Morel's suggested approach was directly to the contrary.³⁵⁴⁶ The court noted that Morel's suggested approach was rejected in the Arista Records³⁵⁴⁷ case. Although acknowledging that Morel's position was apparently adopted by the Ninth Circuit in the Columbia Pictures³⁵⁴⁸ case, the court noted that the Ninth Circuit had done so in a footnote which neither directly addressed the statutory text nor engaged in detailed analysis of the issue, and subsequent court decisions had rejected

³⁵⁴³ Id. at 564-65.

³⁵⁴⁴ Id. at 570-75.

³⁵⁴⁵ Id. at 578-80.

³⁵⁴⁶ Id. at 580-81.

³⁵⁴⁷ Arista Records LLC v. Lime Group LLC, 784 F. Supp. 2d 313, 316-21 (S.D.N.Y. 2011).

³⁵⁴⁸ Columbia Pictures Television v. Krypton Broadcasting of Birmingham, Inc., 106 F.3d 284, 294 & n.7 (9th Cir. 1997).

outright the Columbia Pictures decision, including the McClatchey³⁵⁴⁹ case. Accordingly, the court concluded that any awards of statutory damages against SFP or Getty could not be multiplied based on the number of infringers with whom AFP or Getty might be determined to be jointly and severally liable. Rather, AFP and Getty would, at most, be liable for a single statutory damages award per work infringed.³⁵⁵⁰

AFP and Getty subsequently filed a motion for reconsideration for clarification of what the court meant in its earlier ruling that AFP and Getty would at most be liable for a single statutory damages award per work infringed. Specifically, the court cast the issue on reconsideration as whether Morel could elect to pursue one statutory award per work from AFP alone for its individual pre-kill notice conduct and a separate statutory award for that same work from Getty for its individual post-kill notice conduct.³⁵⁵¹ The court concluded, “as a matter of law, that a plaintiff seeking statutory damages for copyright infringement may not multiply the number of per-work awards available in an action by pursuing separate theories of individual liability against otherwise jointly liable defendants.”³⁵⁵²

The court found that, although the question now before the court was different from the one it addressed in its earlier opinion, the statutory language and legislative intent of Section 504(c), as well as relevant precedent, again exhorted adherence to the same conclusion. The court noted that, under Morel’s reading of the statute, a copyright holder could elect to pursue individual awards against otherwise jointly liable defendants, in a single action, so long as the copyright holder could establish that each or all of those defendants was also individually liable. The court rejected this interpretation of Section 504(c)(1), which provides that a copyright owner “may elect to recover ... an award of statutory damages for all infringements involved in the action, with respect to any one work, for which any one infringer is liable individually, or for which any two or more infringers are liable jointly and severally.” The court determined that, contrary to Morel’s position, the best reading of this provision is that the “or” distinguishes between the two factual scenarios in which a copyright holder would be entitled to recover statutory damages for the infringement of his work, rather than between two types of awards or theories of recovery. Those two factual scenarios are, first, one in which “any one infringer is liable individually,” and, second, one in which “two or more infringers are liable jointly and severally.”³⁵⁵³

Morel urged the court to focus on the interplay between the “or,” and the preceding statutory term, “elect,” arguing that the election the copyright owner is permitted to make is between pursuing an individual or a joint award. The court rejected this, finding the only

³⁵⁴⁹ McClatchey v. The Associated Press, 2007 U.S. Dist. LEXIS 40416

10 (W.D. Pa. June 4, 2007).

³⁵⁵⁰ Agence France Presse, 934 F. Supp. 2d at 581-82.

³⁵⁵¹ Agence France Presse v. Morel, 934 F. Supp. 2d 584, 586 (S.D.N.Y. 2013).

³⁵⁵² Id.

³⁵⁵³ Id. at 589.

supportable reading of the plain language to be that the copyright owner’s election is to recover statutory damages under Section 504(c) in lieu of actual damages and profits under Section 504(b).³⁵⁵⁴ “Because the statutory language of § 504(c) does not establish two categories of awards from which a plaintiff may make an election, whether an award will be individual rather than joint and several is a question of fact not susceptible to the gamesmanship in which Morel is attempting to engage. If a single individual acting alone infringes a work, the award is individual. If multiple infringers acting together infringe a work, the award is joint and several. Nothing in this proposition or in the statutory language permits a plaintiff to make an election that contravenes fact.”³⁵⁵⁵

Finally, the court rejected Morel’s argument that the result should be different where there is a causal or temporal break in the infringement, as here, noting the general statutory intent of Section 504(c) that contemplates a single per-work award for “all infringements involved in the action” – language which does not focus on whether there are causal or temporal breaks in infringement. And in any event, the court ruled that no reasonable jury could conclude that the pre- and post-kill notice conduct constituted separate infringements for which AFP and Getty would not be jointly and severally liable.³⁵⁵⁶

In Nov. 2013, a New York federal jury found that both AFP and Getty had willfully infringed Morel’s copyright in the eight photographs, awarded Morel \$275,000 in actual damages, \$28,889.77 total in infringer’s profits, and \$1.2 million in statutory damages; found that AFP and Getty had jointly committed sixteen violations of the CMI provisions of the DMCA for the distribution of false bylines; and awarded Morel an additional \$20,000 for those DMCA violations. Morel elected to receive statutory damages in lieu of actual damages and infringer’s profits, and the court entered judgment in the total amount of \$1,220,000.³⁵⁵⁷

AFP and Getty then each moved for JMOL on the jury’s finding that they willfully infringed Morel’s copyright in the eight photographs, as well as on the DMCA claims. They also moved in the alternative for a new trial on the jury’s willfulness finding, and for a new trial or remittitur on the jury’s damages award for copyright infringement. The court rejected the motions for JMOL or for a new trial with respect to willfulness, finding the evidence was sufficient for the jury to conclude that both AFP’s and Getty’s infringement was willful under either an actual knowledge or reckless disregard theory.³⁵⁵⁸

With respect to AFP’s DMCA liability, the court ruled that much of the same evidence on which the jury could have found that AFP’s infringement was willful also permitted it to find AFP liable under both Sections 1202(a) and 1202(b). For example, with respect to Section 1202(a),

³⁵⁵⁴ Id.

³⁵⁵⁵ Id. at 590.

³⁵⁵⁶ Id. at 590, 594.

³⁵⁵⁷ Agence France Presse v. Morel, 2014 U.S. Dist. LEXIS 112436 at *7 (S.D.N.Y. Aug. 13, 2014).

³⁵⁵⁸ Id. at *7, *10-18.

the jury could have concluded based on an employee's Twitter activity that he knew the eight images were not Suero's from the beginning yet falsely credited them to Suero. Additionally, even if AFP's addition of the identifier "AFP" to Morel's images did not imply that AFP itself was the copyright owner, there was sufficient evidence that it conveyed false identifying information about the author of the work by implying that Morel was associated with AFP, which he was not. And the jury could have concluded that AFP acted with the required intent by providing and distributing the false CMI in order to license Morel's photographs to its customers. With respect to Section 1202(b), when AFP issued the caption correction identifying Morel as the author, not Suero, it concededly had not received permission from Morel to either distribute his photographs or make the correction. From this evidence, the jury could have concluded that in continuing to distribute the photographs with a caption identifying Morel as the photographer, AFP had both altered the name of the author of the photographs without the authority of the copyright owner, and had distributed Morel's images while knowing that their CMI had been altered without his authority. And the jury could have concluded that AFP knew or had reasonable grounds to know that its alteration of CMI would induce, enable, or facilitate infringement by enabling the continued licensing of Morel's images – which were now credited to Morel but still not AFP's to license – to AFP's customers.³⁵⁵⁹

With respect to Getty's DMCA liability, the court found that the evidence supporting the jury's willfulness finding with respect to Getty's copyright infringement was also sufficient to support its finding that Getty violated Section 1202(a). Specifically, given that a Getty employee knew that the Suero-credited photographs were still available on Getty's feed yet failed to remove them after receiving AFP's kill notice, the jury could have concluded that he did so with the intent to enable the continued licensing of the Suero-credited images to Getty's customers. On that view of the facts, the employee also would have known, at the point when he failed to remove the images from Getty's feed, that CMI associated with the Suero-credited images – the Suero credit and "AFP" and "Getty Images" identifiers – was false. Accordingly, there was sufficient evidence for the jury to conclude that Getty's continued distribution of the Suero-credited images following AFP's kill notice satisfied all of the elements required by Section 1202(a).³⁵⁶⁰

However, the court concluded there was insufficient evidence to find Getty liable under Section 1202(b). The court agreed with the defendants that the addition of the identifiers "AFP" and "Getty Images" could not constitute removal or alteration of CMI, since both of those words suggest that a defendant must take some action with respect to preexisting CMI. On that interpretation, the evidence showed that there were only two ways in which CMI on Morel's photographs was altered or removed without his authority – when Suero first took the images from Morel's feed and removed the identifying information that accompanied the images on that feed, and when AFP changed the photographer credit on the photographs from Suero to Morel. Although Getty itself did not participate in these actions, it might still be liable if it distributed the images knowing that the CMI had been altered or removed without Morel's

³⁵⁵⁹ *Id.* at *20-23.

³⁵⁶⁰ *Id.* at *23-24.

consent. But even if the jury believed that the Getty employee knew there were images on Getty's feed that were wrongly credited to Suero even after AFP's kill notice, there was no evidence that he or anyone else at Getty knew that Suero had removed the CMI from Morel's photographs. And there was no evidence that Getty knew Morel had not given AFP authority to change the photographer credit from Suero to Morel when AFP sent the caption correction; even if that lack of authority could have been inferred from the subsequent kill notice, there was no evidence that Getty continued to distribute Morel-credited images (as opposed to Suero-credited images) post-kill notice.³⁵⁶¹

With respect to statutory damages for the DMCA violations, the defendants argued that Morel could not recover for any DMCA violations because there was insufficient evidence for the jury to conclude that he suffered an injury separate and apart from the injuries attributable to the defendants' copyright violations. The court rejected this argument, noting that the jury was instructed that if it found that Morel was entitled to a verdict on both his copyright infringement and his DMCA claims, it could not compensate him twice for any harm he might have suffered. The court ruled that the jury must therefore be presumed to have determined that Morel suffered additional harm beyond what he suffered as a result of the defendants' copyright infringement. The court also rejected the defendants' argument that even if the jury was correctly instructed, there was insufficient evidence supporting its finding that Morel suffered \$20,000 in actual damages. The court noted that statutory damages can be awarded even in the absence of sufficient evidence supporting actual damages. In light of all the factors the jury was entitled to consider, its statutory award of \$20,000, or half the statutory minimum, was permissible.³⁵⁶²

Finally, the court rejected the defendants' challenges to the statutory damages award for copyright infringement as intrinsically excessive. Under Second Circuit law, statutory damages need not have a direct correlation with actual damages. And in any event, here there was evidence from which the jury could have concluded that the defendants' infringement (and particularly AFP's) was not just willful but reflected a gross disregard for the rights of copyright holders. Accordingly, the court concluded that in the light of all the considerations the jury was entitled to consider, remittitur of the \$1.2 million statutory damages award was not required.³⁵⁶³

The court therefore denied the defendants' motions for JMOL, a new trial, and/or remittitur, except as to Getty on Morel's claim under Section 1202(b), which the court granted. The court altered the jury's award such that AFP and Getty continued to be jointly liable for \$1,210,000 and AFP was individually liable for the remaining \$10,000.³⁵⁶⁴

w. Columbia Pictures v. Fung

³⁵⁶¹ Id. at *24-26.

³⁵⁶² Id. at *28-31.

³⁵⁶³ Id. at *43-47.

³⁵⁶⁴ Id. at *47-48.

In Columbia Pictures Industries, Inc. v. Fung,³⁵⁶⁵ the defendants operated BitTorrent sites through which users could search indexes for dot-torrent files pointing to infringing movies and other content. The district court found the defendants liable for inducement of infringement and rejected assertion of a safe harbor under Section 512(c). The court found the Section 512(c) inapplicable because the defendants' sites were used to download dot-torrent files only, not content files. Because infringing materials did not reside on the defendants' system, the defendants could not rely on Section 512(c).³⁵⁶⁶

On appeal, the Ninth Circuit held that the defendants could not rely on the Section 512(c) safe harbor, but on a different rationale. The Ninth Circuit held that the district court was in error to conclude that the defendants were ineligible for the Section 512(c) safe harbor because the infringing material did not actually reside on the defendants' servers. The court noted that Section 512(c) explicitly covers not just the storage of infringing material, but also infringing activities that use material stored on the system or network. Here, the infringing activity associated with the peer-to-peer transfer of pirated content relied upon torrents stored on the defendants' web sites. Sometimes those torrents were uploaded by users of the sites, while other torrents were collected for storage by the defendants' web sites themselves. The former situation would be at least facially eligible for the safe harbor, assuming the other criteria were met.³⁵⁶⁷

Nevertheless, the court concluded that the defendants were not eligible for the Section 512(c) safe harbor because they satisfied the knowledge, financial benefit, and control prongs of the safe harbor. With respect to the knowledge prong, the court noted that in UMG Recordings v. Shelter Capital, it had endorsed the Second Circuit's interpretation of Section 512(c)(1)(A) in Viacom, that the actual knowledge provision turns on whether the service provider actually or *subjectively* knew of specific infringement, while the red flag provisions turns on whether the service provider was subjectively aware of facts that would have made the specific infringement *objectively* obvious to a reasonable person. The defendants argued they lacked either type of knowledge, because the plaintiffs failed to provide statutorily compliant notification of infringement. The Ninth Circuit concluded that it need not determine the adequacy of the plaintiffs' notification of claimed infringement because the defendants had red flag knowledge of a broad range of infringing activity for reasons independent of any notifications from the plaintiffs. Specifically, the defendants had actively encouraged infringement by urging users to both upload and download particular copyrighted works, providing assistance to those seeking to watch copyrighted films, and help users burn copyrighted material onto DVDs. The material in question was sufficiently current and well-known that it would have been objectively obvious to a reasonable person that the material solicited and assisted was both copyrighted and not licensed to random members of the public, and that the induced use was therefore infringing. Thus, while the defendants' inducing actions did not necessarily render them per se ineligible for

³⁵⁶⁵ 2009 U.S. Dist. LEXIS 122661 (C.D. Cal. Dec. 21, 2009), aff'd, 710 F.3d 1020 (9th Cir. 2013).

³⁵⁶⁶ Id. at *59-60.

³⁵⁶⁷ Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1042-43 (9th Cir. 2013).

the Section 512(c) safe harbor, they were relevant to a determination that the defendants had red flag knowledge.³⁵⁶⁸

The court noted in a footnote that it was not clear from the language of Section 512(c) or from the pertinent case law whether exclusion from the Section 512(c) safe harbor because of actual or red flag knowledge of specific infringing activity applies only with regard to liability for that infringing activity, or more broadly. The court decided it need not reach that issue, because it had also concluded, for the reasons set forth below, that the defendants were not eligible for the safe harbor by virtue of the financial benefit/right to control prongs, and failure of the financial benefit/right to control prongs is sufficient to deny the safe harbor generally for all infringing activity on the web site.³⁵⁶⁹

Turning to the financial benefit and right to control prongs, the court first observed that the statutory language of Section 512(c)(1)(B) sets out as the requirement that the service provider not receive a financial benefit directly attributable to the infringing activity, *then* states the “right and ability to control” language in a dependent clause. Accordingly, the court concluded that the lack of direct financial benefit requirement is central, with the right to control prong being secondary.³⁵⁷⁰

With that as background, the court noted it was an issue of first impression what constitutes a financial benefit *directly* attributable to the infringing activity where the service provider’s revenue is derived from advertising and not from users. The court held that in this case the connection between the infringing activity and the defendants’ income stream derived from advertising was sufficiently direct to meet the financial benefit prong by virtue of the fact that the defendants promoted advertising by pointing to infringing activity, obtained advertising revenue that depended on the number of visitors to their sites, attracted primarily visitors who were seeking to engage in infringing activity, as that is mostly what occurred on their sites, and encouraged that infringing activity.³⁵⁷¹

With respect to the control prong, the court noted that in UMG Recordings it had adopted the Second Circuit’s interpretation in Viacom that in order to have the right and ability to control, the service provider must also exert substantial influence on the activities of users. Here, the defendants’ ability to control infringing activities on their web sites went well beyond merely locating and terminating users’ access to infringing material. The court again noted the defendants’ activities to induce infringement, and stated that, although such inducement actions did not categorically remove them from the Section 512(c) safe harbor, they demonstrated the substantial influence the defendants exerted over their users’ infringing activities, and thereby supplied one essential component of the right to control exception to the Section 512(c) safe

³⁵⁶⁸ Id. at 1043.

³⁵⁶⁹ Id. at 1043 n.20.

³⁵⁷⁰ Id. at 1045.

³⁵⁷¹ Id.

harbor. Accordingly, because the defendants met both prongs of Section 512(c)(1)(B), they were not eligible for protection under the Section 512(c) safe harbor.³⁵⁷²

Lastly, the court observed that it had no difficulty concluding that where the Section 512(c)(1)(B) safe harbor requirements are not met, the service provider loses protection with regard to *any* infringing activity using the service on the following rationale. To satisfy the control prong, there must be substantial influence on the infringing activities of users, indicating that it is the overall relationship between the service provider and infringing users that matters. Also, to the degree the financial benefit/right to control prongs had their origin in vicarious liability concepts, those concepts rest on the overall relationship between the defendant and the infringers, rather than on specific instances of infringement. Accordingly, if the Section 512(c)(1)(B) requirements are met, the entire relationship between the defendant and the infringers should fall outside the safe harbor. The court therefore held that because the defendants did not meet the requirements of Section 512(c)(1)(B), they were outside the Section 512(c) safe harbor with respect to all infringement activities on their sites that were the subject of this suit.³⁵⁷³

After the Ninth Circuit's decision, Fung agreed to a \$110 million judgment and to shut down his web site by Oct. 23, 2013.³⁵⁷⁴

x. Ventura Content v. Motherless

The District Court Decision

The defendants in this case operated a website, Motherless.com, that allowed its users to upload pictures and videos for viewing by others. The pictures and videos were stored on servers rented by Motherless in Texas. The vast majority of pictures and videos available on the site depicted sexually explicit content. The Terms of Use for the site required users to affirm that they had the necessary licenses and permissions to use and authorize Motherless to use all copyright rights in the posted content, and further required users to agree not to post or otherwise distribute or facilitate distribution of any content that infringed any copyright right of any party. The site employed its own review process designed to ensure that uploaded content did not violate its Terms of Use. Within two to four days of submission of a new video, a Motherless employee or representative briefly reviewed five thumbnails automatically created by the system at five equally spaced points in the video for obvious signs of child pornography, copyright notices, watermarks, and any other information that would indicate the video contained illegal content or violated the Terms of Use. No other portions of the videos were

³⁵⁷² *Id.* at 1045-46.

³⁵⁷³ *Id.* at 1046.

³⁵⁷⁴ "Website at Center of Copyright Infringement Action Agrees to Shut Down World Wide," *BNA's Patent, Trademark & Copyright Journal* (Oct. 17, 2013), available as of Oct. 17, 2013 at http://iplaw.bna.com/iprc/display/simple_doc_display.adp?fedfid=37305808&vname=ptdbulallissuesdib&jd=a0e2n9r2f6&split=0#a0e2n9r2f6.

reviewed. Motherless had an “awards” program, through which it recognized the user who uploaded the most viewed content, or who uploaded the most content. Motherless also selected certain content to be prominently featured on the web site.³⁵⁷⁵

The plaintiff was the owner of copyright in 19 films, portions of which had been uploaded by 8 users in 33 clips on the site. The plaintiff made no effort to inform the defendants that the 33 clips contained copyrighted material, instead electing to file suit for copyright infringement. After filing suit, the plaintiff provided the defendants with the URLs of the 33 video clips at issue, and on the same day the defendants deleted the videos from the site. The defendants moved for summary judgment under the Section 512(c) safe harbor, which the court granted.³⁵⁷⁶

The court first determined that the plaintiff had made out a prima facie case of direct infringement against the defendants, because, by allowing users to upload the infringing videos onto its web site, and subsequently allowing other users to access and view those stored videos, the defendants infringed upon the plaintiff’s exclusive right to display its videos. The court did not discuss the volitional requirement for direct infringement, but simply cited the Ninth Circuit’s decision in Perfect 10 v. Amazon for support of its finding.³⁵⁷⁷

The court then considered each of the multiple elements required to establish the Section 512(c) safe harbor. The court first noted that the defendants did not have actual knowledge of the infringements at issue because the plaintiff did not notify them that its copyrighted material was available on the web site, and the plaintiff had not otherwise submitted evidence that they had specific knowledge of particular infringing material.³⁵⁷⁸

The court then turned to whether the defendants had red flag knowledge. The court noted that, under the Ninth Circuit’s decision in UMG Recordings, Inc. v. Shelter Capital Partners, LLC,³⁵⁷⁹ the difference between actual and red flag knowledge is between a subjective and an objective standard. Actual knowledge turns on whether the service provider actually or subjectively knew of specific infringement, whereas red flag knowledge turns on whether the provider was subjectively aware of facts that would have made the specific infringement objectively obvious to a reasonable person. Like the actual knowledge requirement, the red flag test applies only to specific instances of infringement.³⁵⁸⁰

The court found that the plaintiff had failed to produce any evidence whatsoever from which it might infer that the defendants were aware of facts or circumstances indicating the clips at issue were infringing. The plaintiff cited the Ninth Circuit’s suggestion in Shelter Capital that a

³⁵⁷⁵ Ventura Content, Ltd. v. Motherless, Inc., 2013 U.S. Dist. LEXIS 189948 at *2-6 (C.D. Cal. July 3, 2013).

³⁵⁷⁶ Id. at *1, 6.

³⁵⁷⁷ Id. at *9-10.

³⁵⁷⁸ Id. at *16-17.

³⁵⁷⁹ 718 F.3d 1006 (9th Cir. 2013).

³⁵⁸⁰ Motherless, 2013 U.S. Dist. LEXIS at *18.

DMCA-compliant notice from a *third party* copyright holder might confer red flag knowledge upon a service provider. The plaintiff pointed to three instances in which the defendants took between 10 to 15 days to remove copyrighted material identified by a third party copyright holder in response to DMCA-compliant notices. The court ruled that, even assuming that such third party notices could be considered in evaluating red flag knowledge, the three lapses in prompt takedown cited by the plaintiff could not alter the court's conclusion that the defendants were entitled to the Section 512(c) safe harbor. The undisputed facts established that the defendants expeditiously removed the vast majority of infringing material upon receipt of over 3,500 DMCA-compliant notices and that was sufficient to qualify for the safe harbor.³⁵⁸¹

The court then rejected four additional argument made by the plaintiff that it asserted raised a genuine issue of material fact as to actual or red flag knowledge:

-- The plaintiff contended that the defendants "must" have known that infringing material had been uploaded onto their web site because their business model was reliant on mass infringement, supposedly based on the fact that pornography-only web sites attract visitors by holding a large amount of free material, and the only way to accumulate a large volume of free pornography is to get large volumes of professionally created pornography uploaded by users. The court rejected this argument, noting that the safe harbor requires expeditious removal of material only once a service provider gains actual or red flag knowledge, and there was no genuine dispute of material fact that the defendants expeditiously removed infringing material upon gaining actual or red flag knowledge of specific instances of infringement. And the safe harbor does not require the defendants, as the plaintiff suggested, to offer evidence of content subject to copyright protection but lawfully available on its systems, such as videos created by users or videos that the defendants provided pursuant to arrangements they reached with major copyright holders. A service provider does not have the burden to demonstrate that material on its web site was *not* copyright-infringing, as Congress elected to place the burden of policing copyright infringement on the owners of the copyright. Finally, the court noted that, had the defendants' business model truly been reliant on mass infringement, the plaintiff should have been able to unearth a substantial amount of copyrighted content that remained on the web site well after the defendants received DMCA-compliant notices, and the plaintiff had found only three such instances.³⁵⁸²

-- Next the plaintiff contended that groups on the Motherless site named for professional porn stars, celebrities or copyrighted movies showed that the defendants encouraged the uploading of infringing material. The court rejected this argument, noting that, just as permitting users to "tag" their content to a group named "music videos" was insufficient in Shelter Capital to demonstrate actual or red flag knowledge, allowing users to "group" their content under the identified categories was insufficient to establish the required knowledge here. The plaintiff had failed to offer evidence that the content tagged to a particular group actually displayed images of the celebrities, television shows, or porn stars for which the groups

³⁵⁸¹ Id. at *20-21 & n.5.

³⁵⁸² Id. at *22-27.

were named. And the fact that the defendants gave out rewards to those users who uploaded the most content, or the most popular content, did not demonstrate actual or red flag knowledge of specific instances of infringement, but rather proved only that the defendants were encouraging uploading. Similarly, the fact that the defendants placed popular content where it was most likely to be seen, and chose certain content for prominent locations, demonstrated only that the defendants were attempting to increase their revenue, not that they knew specific content highlighted was infringing.³⁵⁸³

-- The plaintiff also argued that the professional nature of the content on the Motherless site demonstrated that the defendants knew or were aware of specific instances of infringement. The court rejected this argument, noting that the professional nature of submitted content does not per se constitute a red flag – given the audiovisual equipment available to the general public today, there may be little, if any, distinction between professional and amateur productions.³⁵⁸⁴

-- Finally, the plaintiff argued that the defendants must have known their users were uploading copyrighted material because their employees reviewed and approved all uploads, many of which contained watermarks or other express indicia of ownership. The court initially noted skepticism about whether it would be proper to rule that actual or red flag knowledge can be gained merely by reviewing content uploaded onto a web site for the express purpose of determining whether such content is infringing. Such a rule would, in effect, penalize a service provider for taking measures designed to prevent copyright infringement. Furthermore, it would have the impermissible effect of shifting the burden of determining whether specific content was illegal onto the service provider. The court refused to rely on evidence submitted by the plaintiff's expert that, of 996 clips uploaded to the site that he reviewed over an eleven-hour time span, 66.3% of them were watermarked or contained other information identifying the content producer, and an additional 20.3% of them were professionally produced or obviously proprietary. The court found several flaws in this evidence. First, the expert reviewed the clips as they were being uploaded by users, but his study did not indicate how many of the 996 clips remained on the site after the defendants screened them. Second, his study failed to specify where the watermarks or other indicia of ownership appeared on each clip, and therefore did not prove whether they were within the five thumbnails captured by the defendants' system for each video for use by its reviewers. Third, the expert did not identify what the watermarks or other indicia of ownership were, such that, had the defendants reviewed the clips and seen the indicia, it would have been apparent that the material was infringing.³⁵⁸⁵

The court then turned to whether the defendants exhibited willful blindness to infringement on their web site. Although the plaintiff had made no argument that the defendants willfully buried their head to infringement, the court concluded the record contained no evidence the defendants acted in that manner, given the undisputed evidence that they had

³⁵⁸³ Id. at *27-30.

³⁵⁸⁴ Id. at *30-31.

³⁵⁸⁵ Id. at *31-35.

received over 3,500 takedown notices and that in response to both compliant and non-compliant notices, they had automatically deleted the identified content.³⁵⁸⁶

The court then turned to the issue of whether the defendants had the right and ability to control infringing content and concluded that they did not. Under Shelter Capital, the service provider must exert substantial influence on the activities of users, which may include high levels of control over activities of users or purposeful conduct. Here there was evidence only that the infringing material resided on the defendants' system and the defendants had the physical ability to remove the content. The plaintiff had submitted no other evidence raising a genuine issue of material fact as to whether the defendants exerted substantial influence on the activities of its users. The mere fact that the defendants had a Terms of Use and enforced them by removing material and terminating users who violated those terms did not defeat the safe harbor.³⁵⁸⁷

The court then analyzed the defendants' policy for termination of repeat infringers. The plaintiff conceded that Motherless had adopted an adequate termination policy, informed its subscribers of it, had a working notification system and procedures for dealing with DMCA-compliant notices, did not actively prevent copyright owners from collecting information needed to issue notices, and sufficiently tracked users with a history of infringing. The plaintiff argued, however, that the defendants had not reasonably implemented that policy by failing to terminate repeat infringers in appropriate circumstances. The defendants submitted undisputed evidence that they had terminated between 1,300 and 2,000 users for alleged copyright infringement, in response to which the plaintiff identified nine users – the eight users who uploaded the 33 clips at issue and one other user – it alleged were repeat infringers who should have been terminated but were not. The court ruled that, even assuming the defendants should have terminated those users, the defendants' failure to do so did not raise a triable issue of fact as to whether defendants reasonably implemented their termination policy. The DMCA requires only that the policy be reasonably – not perfectly – implemented, so occasional lapses are not fatal.³⁵⁸⁸

In any event, of the nine users identified by the plaintiff, the defendants had no evidence that three of them had previously uploaded infringing content before the suit, had evidence of only a single infringement by three others, and had evidence one had infringed twice before. Thus, although four of these users were arguably "repeat" infringers, their infringement was in no way blatant or flagrant, thus excusing the defendants' failure to terminate them. And as to one of the nine users, the defendants had received only one notice that it had uploaded 21 infringing works. The court noted that a service provider's failure to terminate users who upload multiple videos that are identified in a single DMCA notice does not remove Section 512(c)'s immunity. In sum, out of more than 700,000 users who had been active on the site since its inception, the plaintiff had identified only one who was arguably allowed to remain on the site despite evidence that it had repeatedly and blatantly uploaded infringing activity. The court

³⁵⁸⁶ Id. at *36.

³⁵⁸⁷ Id. at *38-40.

³⁵⁸⁸ Id. at *42-44.

therefore concluded that the defendants had reasonably implemented their termination policy.³⁵⁸⁹

Based on its analysis, the court granted summary judgment that the defendants were entitled to the Section 512(c) safe harbor, and ruled that because the defendants had already removed the 33 infringing clips at issue, the plaintiff's request for injunctive relief was moot.³⁵⁹⁰

The Ninth Circuit's Decision

On appeal, the Ninth Circuit affirmed.³⁵⁹¹ The court noted the following facts about operation of the site that seemed key to its rulings, both specifically and contextually:

-- Each time a user uploaded a file, he received a warning on his computer screen stating, "Anyone uploading illegal images/videos will be reported to the authorities. Your IP address ... has been recorded. Any images/videos violating our Terms of Use will be deleted."³⁵⁹²

-- Motherless did not edit, review, or approve file names, titles, or tags, although it did maintain links to certain classes of content, such as "Most Viewed" and "Most Popular."³⁵⁹³

-- The site's Terms of Use prohibited posting copyrighted material without the prior written consent of the copyright owner and invited takedown notices for infringing material. Motherless also used a software program that provided copyright owners with a link and password so that they could directly delete infringing material themselves, without having to send a takedown notice.³⁵⁹⁴

-- Upon upload, software generated a thumbnail of each picture, and five thumbnails of each video clip at the 20%, 40%, 60%, 80% and 100% time points in the clip. Joshua Lange, the founder of the site, or his contractor looked at each thumbnail for obvious signs of child pornography, copyright notices, watermarks, and any other information that would indicate the material contained illegal content or violated the Terms of Use. Lange spent three to six hours a day, seven days a week, looking at the uploads and estimated he reviewed 30,000 to 40,000 images per day.³⁵⁹⁵

-- Lange personally examined all copyright infringement notices, whether DMCA-compliant or not, and deleted any infringing content he could find. He deleted material

³⁵⁸⁹ Id. at *44-49.

³⁵⁹⁰ Id. at *49-50.

³⁵⁹¹ Ventura Content, Ltd. v. Motherless, Inc., 885 F.3d 597 (9th Cir.), cert. denied, 139 S. Ct. 419 (2018).

³⁵⁹² Id. at 601.

³⁵⁹³ Id.

³⁵⁹⁴ Id.

³⁵⁹⁵ Id.

identified as infringing by a complainant ordinarily within a day or two. Motherless used software to prevent users from re-uploading previously deleted material. Lange had deleted over 4.5 million pictures and videos for violating Motherless's Terms of Use and estimated that 4%-6% of the deleted files were for copyright infringement.³⁵⁹⁶

-- Motherless did not have a written policy instructing its employees on when to expel repeat infringers because there were no employees to instruct. Termination was a matter of Lange's judgment. He considered the following factors in deciding whether to terminate a repeat infringer: (1) the volume of complaints; (2) the amount of linked content in the complaints; (3) the timespan between notices; (4) the length of time the alleged infringer's account had been active; (5) the amount of total content the account had; (6) whether the user was maliciously and intentionally uploading infringing content or uploading content without knowing the source; and (7) whether the takedown notices were DMCA-compliant. Between 2008 and 2011, Lange terminated over 33,000 user accounts for violating the website's Terms of Use and estimated that he terminated about 4%-6% of the users for possible copyright infringement, which would have been between 1,320 and 1,980 users.³⁵⁹⁷

-- There were no Ventura watermarks, credits, or other pieces of information suggesting in any way that Ventura owned the copyright in the movies from which the allegedly infringing 33 posted clips were taken. Ventura did not send DMCA notices or any other sort of takedown notice for the infringing material, nor did it remove the material itself as Motherless's software link enabled it to do.³⁵⁹⁸

The Ninth Circuit rejected all of the reasons proffered by Ventura for why the defendants should not be entitled to 512(c) safe harbor. First, Ventura argued that material on Motherless should not be considered stored at the direction of users because Lange uploaded 700,000 files from a previous website, screened uploads for illegal material before putting them on the site, and had software categorize material into classes, such as "Most Popular." The court rejected this, noting that Lange had not uploaded any material to the site since he started it with his old material and there was no evidence any of that material was infringing. Nor did Lange or his contractors upload any of the 33 clips over which Ventura claimed ownership. With respect to screening of posted material, the court noted that Section 512(m) says the law should not be construed to eliminate the safe harbor because a service provider monitors for infringement or disables access to material where the conduct depicted is prohibited by law. The court could not imagine that Congress intended to deprive a web site of the safe harbor because it screened out child pornography and bestiality rather than displaying it.³⁵⁹⁹

³⁵⁹⁶ Id.

³⁵⁹⁷ Id. at 601-02.

³⁵⁹⁸ Id. at 602.

³⁵⁹⁹ Id. at 604-05.

The court found its decision in UMG v. Shelter Capital Partners case to be controlling here, as did the district court. As in that case, Motherless’s users, not the web site, decided what to upload and what file names and tags to use. Under Shelter Capital, altering the file format to make it accessible before posting, enabling users to apply search tags to uploads, and facilitating user access to files that other users posted, do not deprive a web site of safe harbor protection. Nor did Motherless’s use of software to highlight the “Most Popular” material deprive it of the safe harbor because Motherless did not screen out material for relatively low popularity. And the court did not see why the Motherless incentive program, which made credits usable to buy coffee mugs and T-shirts for high volume uploaders, make “storage” at the direction of Motherless rather than its users.³⁶⁰⁰

The court distinguished its decision in Mavrix Photographs, LLC v. LiveJournal, Inc.,³⁶⁰¹ on the ground that in Mavrix there was a genuine issue of fact as to whether the web site’s moderators who reviewed user submissions for relevance to new and exciting celebrity news were agents of the web site. By contrast in the present case, Lange and his contractors did not review whether the pornography submitted by users met any discretionary standards. Lange’s editing was limited to the kind protected by Section 512(m), screening out illegal material.³⁶⁰²

The court then turned to issues of knowledge under the safe harbor. Ventura argued that Lange must have had actual knowledge the Ventura clips were infringing because a few had watermarks and they appeared to be professionally produced. The court rejected this argument. Only four of the clips had watermarks and they were not in the name of Ventura, but rather of sites suggesting they came from pornography aggregators rather than copyright owners. The court noted that professionally created work is often posted online to publicize and attract business for the creator. Amateurs often do professional quality work in artistic endeavors, and amateurs are no less entitled to copyright protection than professionals, so it was not apparent why professionalism should matter. And digital cameras have become so good and so easy to use that even home movies of children’s birthday parties can look professionally done. The court also noted that Ventura had made no effort to give Motherless actual knowledge of infringement through watermarks or DMCA notices. Ventura had therefore failed to establish a genuine issue of fact as to actual knowledge of infringement.³⁶⁰³

Nor had Ventura established red flag knowledge, given that its arguments for that type of knowledge were similar to its arguments for actual knowledge, and there was nothing about the Ventura clips that would make infringement apparent. The Ninth Circuit noted its agreement with the Second Circuit’s holding in Capitol Records, LLC v. Vimeo, LLC³⁶⁰⁴ that, even if it were obvious to a reasonable person that some of the material on the site must be infringing, for

³⁶⁰⁰ Id. at 605-06.

³⁶⁰¹ 718 F.3d 1006 (9th Cir. 2013).

³⁶⁰² Motherless, 885 F.3d at 606-07.

³⁶⁰³ Id. at 608-09.

³⁶⁰⁴ 826 F.3d 78 (2d Cir. 2016).

purposes of the safe harbor it must be obvious that *the particular material that is the subject of the claim* is infringing. Here, it would not be obvious to a reasonable person that the clips excerpted from Ventura movies were infringing for the reasons noted. Nor was there any record of Motherless actively encouraging infringement by urging users to upload and download particular copyrighted works. To the contrary, Lange estimated he had deleted over 180,000 videos and pictures for copyright infringement, and had removed an estimated 1,320 to 1,980 users from the site for repeated copyright infringement. And software used on the site stopped users from re-uploading previously deleted material. Ventura therefore failed to establish red flag knowledge.³⁶⁰⁵

With respect to expeditious takedown, the court noted that Ventura had not sent Motherless a DMCA notification before filing suit. When Lange was served with Ventura's complaint, he twice asked Ventura for the URLs to the infringing clips. Upon receiving the URLs, he deleted the 33 infringing clips the same day. The court ruled that such action satisfied Motherless's obligation to respond expeditiously to remove infringing material.³⁶⁰⁶

The court then turned to whether Motherless had the right and ability to control the infringing activity, and if so, whether it received a financial benefit directly attributable to the infringing activity. The court began by noting that the right and ability to control prong involves something more than the ability to remove or block access to materials posted on a service provider's web site. The service provider must be able to exert substantial influence on its users' activities. Here, nothing in the record suggested that Motherless told its users what to upload. It did not curate uploaded content in any meaningful way, nor did it reject unpopular groups or content. It rewarded uploaders of the most popular content with points redeemable for items of negligible value, such as coffee mugs and T-shirts, but that did not amount to encouraging uploads of infringing material. Even after Motherless started letting users exchange points for cash, the payouts were nominal. One of the most prolific uploaders of over 300,000 files testified that he made just \$200. Motherless did not advertise itself as a place to get pirated materials. Although the more pornography Motherless had, the more users it would attract and therefore more advertising revenue, the statute requires financial benefit that is *distinctly attributable to the infringing material at issue*. There was no evidence that Motherless made any money directly from the Ventura clips.³⁶⁰⁷

The court next turned to the safe harbor's requirements for termination of repeat infringers. The court first observed that both it and the Second Circuit agree that subsection (c) of Section 512 is directed to individual infringements, not the service as a whole, setting out what a service provider must do to avoid liability for the infringement of *the copyrighted material at issue*. If subsection (c) were read to apply to all the material on the web site, instead of the material for which a remedy was sought by the victim of infringement, then no large site would be protected by the safe harbor, because it is unimaginable that any web site with

³⁶⁰⁵ Motherless, 885 F.3d at 609-12.

³⁶⁰⁶ Id. at 612.

³⁶⁰⁷ Id. at 613.

hundreds of thousands or millions of user uploads could successfully screen out all of the copyright infringing uploads, or even all of the uploads where infringement was apparent.³⁶⁰⁸

By contrast, the repeat infringer policy requirement of Section 512(i) does not focus on just how the site responds to notice of a particular infringement, but instead addresses how the site is generally managed. Section 512(i)(1)(A) bars use of the 512(c) safe harbor unless the service provider adopts and reasonably implements a policy of terminating repeat infringers in appropriate circumstances. And Section 512(i)(1)(B) requires that the service provider accommodate and not interfere with standard technical measures that enable copyright owners to establish some technical means so that service providers can spot and exclude infringing material without substantial expense. The court noted that, although Section 512(i)(1)(B) was not an issue in this case, one could imagine a digital version of the old c in a circle (©) automatically triggering the uploading software to exclude material so marked by the copyright owner. Here, Ventura had chosen not to mark its material in any way so that infringement could be spotted and the material excluded by some standard technical measure.³⁶⁰⁹

Motherless had a written policy of excluding infringing material, as stated on its membership sign-up page, which required users to represent that they own or have the necessary licenses and consents to use and authorize Motherless to use all copyright rights in submitted content and would not post any content that infringes copyright, and stated that Motherless reserved the right in its sole discretion to refuse, delete, move or edit any content it deemed in violation of law, including copyright law. Motherless also had a written policy of terminating repeat infringers.³⁶¹⁰ On its page titled “DMCA Notice & Takedown Policy and Procedures,” Motherless stated that “[it] is the firm policy of the [site] to terminate the account of repeat copyright infringers, when appropriate.”³⁶¹¹ The court noted that the details of the termination policy were not written down, but the statute does not require that the details be written, just that the site inform subscribers of a policy of terminating repeat infringers in appropriate circumstances. The court noted that a company might need a written policy to tell its employees or independent contractors what to do if there were a significant number of them, but Motherless was not such a firm, given that it consisted only of Lange and a few contractors, and Lange alone determined when to terminate repeat infringers. So the lack of a detailed written policy was not by itself fatal to safe harbor eligibility, nor was the fact that Motherless did not publicize its internal criteria.³⁶¹²

The court then turned to Lange’s description of how he applied Motherless’s repeat infringer policy in his deposition testimony. He testified that he excluded infringing material by looking for an identifying watermark in the corner. If he received a DMCA takedown notice, he

³⁶⁰⁸ Id. at 614.

³⁶⁰⁹ Id. at 614-15.

³⁶¹⁰ Id. at 615.

³⁶¹¹ Id.

³⁶¹² Id. at 615-16.

also used hashing software so that copies of the image or clip would be removed and screened out if anyone tried to post them again. Ordinarily, he would not terminate a user because of one takedown notice, but would if there were two or more. He might make a “gut decision” to terminate a user after the first DMCA notice if there were multiple infringing pictures or videos identified in the notice, though that was not his usual practice. Although Motherless had received over 3,000 DMCA takedown notices, Lange did not keep a written list of subscribers whose submissions generated DMCA notices. Instead, he saved each of the takedown notices and could track the number of times each user’s content had been deleted in response, as well as the date and reason (e.g., copyright infringement, child pornography) for each deletion. In deciding to terminate a user, he considered the account’s history, his memory and judgment, the number of complaints arising from the user’s uploads, the amount of infringing content in the complaint he received, and whether he thought the user had maliciously or intentionally uploaded infringing content.³⁶¹³

The court then noted the various factors that courts have considered as bearing on whether a servicer has reasonably implemented its policy for termination in appropriate circumstances of repeat infringers. Factors that work in favor of the service provider include a DMCA log, blocking a subscriber’s name and email address from uploads, putting email addresses from terminated accounts on a banned list, and prohibiting a banned user from reopening a terminated account. Factors that cut against the service provider include changing the email address to which takedown notices are sent without providing notice of the change, participating in copyright infringement, allowing terminated users to rejoin the site, and refusing to terminate known repeat infringers. The court specifically noted that Congress did not require that, to be eligible for safe harbor, a provider must maintain a logbook of infringers which it consults whenever it receives a DMCA notice, although the use of such a logbook would be good evidence of reasonable implementation of a policy.³⁶¹⁴

Here, the court concluded that no trier of fact could conclude from the evidence in the record that Motherless had failed to reasonably implement a repeat infringer policy. Safe harbor eligibility does not require perfection, just reasonable implementation of the policy in appropriate circumstances, and here there was a paucity of proved failures to terminate. The evidence showed that Motherless terminated between 1,320 and 1,980 users for alleged copyright infringement and that only nine alleged repeat infringers had slipped through, suggesting that less than one repeat infringer in 100,000 active users was missed. The court noted it might be tempting to say that a policy is not reasonably implemented if it does not include both a database of users whose uploads have generated DMCA notices and some automated means of catching them if they do it again. But the statute does not require that – it modifies the termination requirement with the phrase “appropriate circumstances” in addition to the word “reasonable.” Although the dissent in the case pointed out that anonymous users could also upload files, 85% of the uploads came from members, and the Ventura clips were not uploaded by anonymous users. The number of repeat infringers who escaped termination, at

³⁶¹³ *Id.* at 616-17.

³⁶¹⁴ *Id.* at 617-618.

least the record showed, was a tiny number and a minuscule percentage of users. The court observed that doubt that Motherless really did have a policy of terminating repeat infringers that was reasonably implemented was unavoidable in the light of unsystematic and casual implementation. But doubt is not evidence, and Ventura had presented no evidence to establish a genuine issue of fact as to whether Motherless failed to reasonably implement its policy. Accordingly, the court held that Motherless and Lange were entitled to claim the protection of the safe harbor.³⁶¹⁵

y. Disney Enterprises v. Hotfile

In Disney Enterprises, Inc. v. Hotfile Corp.,³⁶¹⁶ Hotfile operated an online storage locker service that enabled users to upload files for storage through a simple user interface. Once a file was uploaded, the user automatically received one or more unique URL links containing the file name and an extension. The link generally gave some indication of the file name and thus its possible content. Although Hotfile provided no index or search feature, it encouraged users to share file links through an affiliate program, which paid individuals to navigate prospective downloaders to file locations. The incentives increased with the size of the file and the frequency of its download but without regard to the content of the file. Hotfile's affiliates created their own web sites that catalogued files found on Hotfile, promoted their files, or allowed the public to search for files. Uploading users could themselves broadcast the download links, such as by emailing them or by advertising them through other channels. Thus, in addition to a storage site, Hotfile had been turned into a file distribution network. Hotfile did not review what its users were uploading, downloading or promoting. Although Hotfile was accessible to the public and anyone could upload or download for free, paying nine dollars per month for "premium" status permitted uploaders to store their files for a longer period; otherwise, files were automatically deleted every three months.³⁶¹⁷

The plaintiffs brought claims for inducement, contributory and vicarious liability against Hotfile and filed a motion for summary judgment seeking an adjudication that Hotfile's activities were not entitled to the DMCA safe harbors.³⁶¹⁸ In support of their motion, the plaintiffs argued that Hotfile did not reasonably implement a repeat infringer policy and the court agreed based on a number of considerations. While noting that the statute does not require a perfect policy or anything as stringent as the three-strikes policy that Hotfile eventually implemented, Hotfile had no way to keep track of infringing users based on infringement notices – it had no technology to record or track notices, no procedure for dealing with notification, and did not base its repeat infringer policy on how many notices were associated with certain users (such as by flagging them). As a consequence, when Hotfile received notices of infringement, it was

³⁶¹⁵ Id. at 618-19.

³⁶¹⁶ 2013 U.S. Dist. LEXIS 172339 (S.D. Fla. Sept. 20, 2013). In an earlier opinion, discussed in Section II.A.4(r) above, the court granted Hotfile's motion to dismiss the plaintiffs' claims of direct infringement, but denied its motion to dismiss with respect to the plaintiffs' claims of inducement, contributory and vicarious liability.

³⁶¹⁷ Id. at *6-11.

³⁶¹⁸ Id. at *5-6.

Hotfile's practice to largely ignore them rather than act to terminate the users they were associated with. Despite receiving over eight million notices for five million users, Hotfile terminated only 43 users before the commencement of the lawsuit. By the time of the lawsuit, 24,790 users had accumulated more than three notices; half of those had more than 10 notices; half again had 25 notices; 1,217 had 100 notices, and 61 had more than 300 notices each. While those who were the subject of more than three infringement notices made up less than one percent of all of Hotfile's users, they were responsible for posting 50 million files (15.6 million of which were subsequently the subject of a takedown notice or removed for infringement), representing 44 percent of all files ever uploaded to Hotfile.³⁶¹⁹

Although noting a split in authority on whether infringement notices alone are sufficient to make a service provider aware of a user's blatant, repeat infringement, the court noted that in this case, the scale of the notices and complaints from copyright holders indicated to Hotfile that a substantial number of blatant repeat infringers made the system a conduit for infringing activity. Yet Hotfile did not act on receipt of DMCA notices and failed to devise any actual policy of dealing with those offenders. The court noted that Hotfile presented no evidence to show that the small number of removals that did occur before the lawsuit were for any reason other than threatened litigation or by court order in lawsuits filed by other plaintiffs. In fact, Hotfile was unable to point to a single specific user who was terminated pursuant to its repeat infringer policy before the complaint was filed, which consisted of manual review and exercise of discretion. Thus, there was never any realistic threat of termination to Hotfile's users, whose activities were protected by the company's indifference to infringement notices. Accordingly, the court ruled that Hotfile was not entitled to the DMCA safe harbor for infringing activity taking place through its site before the lawsuit.³⁶²⁰

After the lawsuit was filed, Hotfile adopted and began to implement a three-strikes policy, resulting in the termination of over 20,000 users based on application of newly adopted fingerprinting and hashing technology. Based on this, Hotfile moved for partial summary judgment on the applicability of the safe harbor to conduct occurring after the litigation was commenced. The court noted that Hotfile's request raised questions of whether a party can ever regain the protections of the DMCA, whether the court should trust Hotfile not to revert to its offending conduct, whether the court could determine the exact point at which Hotfile implemented a DMCA-compliant policy and, if so, whether the court should use the date of technical compliance as the point of entry to the safe harbor or whether the proper measure should be when Hotfile ceased to be a hotbed for infringement. The court decided, however, that it need not adjudicate those issues because the plaintiffs had made clear that they had brought suit based on Hotfile's system and business model as they existed before the complaint and that post-complaint damages were not part of this dispute.³⁶²¹

³⁶¹⁹ Id. at *33-34, *68-70.

³⁶²⁰ Id. at *70-72, *76-81.

³⁶²¹ Id. at *79-81.

Although concluding that Hotfile was not entitled to the safe harbor because of its failure to reasonably implement a repeat infringer policy, the court went on to address two other bases the plaintiffs alleged disqualified Hotfile from the safe harbor – registration and notification of a copyright agent and red flag knowledge. With respect to the first, Hotfile had a “report abuse” form on its web site and provided an email address where users could report infringing content. It did not register a DMCA agent with the Copyright Office until December 2009, did not identify an agent on its web site until May 2010, and had not provided a proper mailing address for its registered agent insofar as it listed only a post office box. Based on these facts, the court concluded that Hotfile would be ineligible under Section 512(c)(2) at least through May 2010, the date on which it published its agent’s contact information, leaving open the question whether the failure to provide a full address and not a post office box, as required by Copyright Office regulations at 37 C.F.R. § 201.38(c) for purposes of registration of an agent, would also disqualify the safe harbor.³⁶²²

With respect to the issue of red flag knowledge, the court decided that the testimony, documents and evidence submitted created an issue of fact for a jury as to whether Hotfile knew or blinded itself to actual infringement of particular works on a small or large scale. Hotfile’s policy prior to the litigation to store only a master file copy when multiple copies of the same file were uploaded by users could mean that Hotfile was attuned to the infringing nature of files, but merely disabled the offending link rather than removing the file itself. Because a significant number of the DMCA notices concerned the plaintiffs’ works, a jury could conclude that Hotfile understood that it was continuing to make particular infringing content available to the public or that, at the very least, it should have investigated those files. Similarly, to the extent that communications with users should have alerted Hotfile to the infringing nature of files on its system that were owned by the plaintiffs (such as users seeking technical assistance who indicated that their difficulties were owing to the illegal nature of their activity), Hotfile might be deemed to have possessed red flag knowledge. A jury would need to resolve these issues of material fact.³⁶²³

In Dec. 2013, the MPAA announced a settlement under which the district court had awarded damages of \$80 million to the plaintiffs and ordered Hotfile to either shut down its operations or use digital fingerprinting technology to prevent copyright infringement by its users.³⁶²⁴

z. Capitol Records v. Vimeo

The District Court’s Decisions

³⁶²² *Id.* at *81-84.

³⁶²³ *Id.* at *87-90.

³⁶²⁴ “Hotfile To Pay \$80M to MPAA, Studios In Copyright Suit,” *Law360* (Dec. 3, 2013), available as of Dec. 7, 2013 at http://www.law360.com/ip/articles/493076?nl_pk=be5fde4e-8dc1-4d81-b621-f0352bcdff74&utm_source=newsletter&utm_medium=email&utm_campaign=ip.

In this case, the defendant Vimeo operated a video sharing platform that required users to upload only videos that they created, or at least participated in creating. Users were required to register with a user name, password and email address in order to upload videos to Vimeo's web site. Several record company plaintiffs sued Vimeo for direct, contributory and vicarious copyright infringement based on 199 videos appearing on the site that contained music from the plaintiffs' copyrighted recordings. The parties filed cross motions with respect to Vimeo's eligibility for the Section 512(c) safe harbor. The court denied summary judgment to Vimeo with respect to 10 employee-uploaded videos and with respect to 55 videos with which Vimeo employees interacted, and granted summary judgment to Vimeo with respect to the remaining videos in suit.³⁶²⁵

With respect to a repeat infringer policy, from the time of Vimeo's inception, Vimeo required users to agree to its Terms of Service, which contained language requiring users not to use the web site to infringe any copyright or other proprietary rights and warning users that Vimeo reserved the right to remove videos and terminate user accounts for violations of the Terms of Service. At some point after its inception, Vimeo began to employ a three strikes rule whereby it would terminate a user's account if the user became the subject of three separate, valid takedown notices. Under this policy, takedown notices received within three days of one another were treated as a single instance of infringement. The email address associated with the terminated account was added to a list of banned email addresses that could not be used in connection with a new account. In addition, when Vimeo reviewed a user account pursuant to a takedown notice that identified allegedly infringing content in a video, it also reviewed the other videos in that user's account for additional violations of the Terms of Service. Any video that was removed pursuant to a takedown notice was placed on a blocked video list, which prevented any Vimeo user from re-uploading the same video file. In October 2008, Vimeo began utilizing a "Purgatory Tool," which facilitated the tracking of repeat infringers by collecting and maintaining all videos and accounts removed from the web site, including those removed because of DMCA takedown notices. A video that was in Purgatory was no longer accessible to anyone except Vimeo employees with moderator status. When a user account was placed in Purgatory, all of that user's videos were automatically placed in Purgatory as well.³⁶²⁶

The court held that these facts were adequate to establish that Vimeo had adopted a policy providing for the termination of access for repeat infringers. The court also found that Vimeo had adequately informed its users of the policy, rejecting the plaintiffs' argument that Vimeo had not communicated to its users a specific "repeat" infringer policy until 2011, when its more specific policy with respect to the handling of repeat infringers was published to its web site. The court ruled that Vimeo's communication of a more general policy – threatening

³⁶²⁵ Capitol Records, LLC v. Vimeo, LLC, 972 F. Supp. 2d 500, 505-07 & 537 (S.D.N.Y. 2013), aff'd in part & vacated and remanded in part, 826 F.3d 78 (2d Cir. 2016).

³⁶²⁶ Id. at 511-12.

account termination upon any violation of the Terms of Service including single or repeated instances of infringement – from its inception sufficed.³⁶²⁷

The court then ruled that Vimeo’s repeat infringer policy had been reasonably implemented. In its nascent years, Vimeo employees identified repeat infringers by reviewing email records or recalling the names of users previously implicated in a takedown notice. User accounts violating the Terms of Service were often terminated upon the receipt of the first DMCA takedown notice. As Vimeo grew in size and the number of takedown notices received per month increased, Vimeo’s policy became more robust – first in the form of a three strikes rule and a blocked video list, and eventually in the form of the Purgatory tool.³⁶²⁸ “That Vimeo’s enforcement mechanisms advanced in step with the realities of its growing business further supports the reasonableness of its implementation system.”³⁶²⁹ The court rejected the plaintiffs’ argument that Vimeo’s policy of blocking only the email address of a repeat infringer was insufficient because it allowed a repeat infringer to set up another account using a different email address. Nor was Vimeo required to block by IP address in order to establish reasonableness. The court also rejected the plaintiffs’ challenge to Vimeo’s policy to treat all notices received within a three day period as a single instance of infringement, finding such treatment to be reasonable.³⁶³⁰

Although the plaintiffs did not expressly argue that Vimeo failed to meet the requirement that it not interfere with standard technical measures used by copyright owners to identify or protect copyrighted works, the court noted that the plaintiffs did claim that Vimeo’s privacy settings prevented copyright owners from collecting information needed to issue a takedown notice. Even if true, the court found such fact insufficient to demonstrate failure to meet the non-interference with standard technical measures requirement. Apart from the fact that the plaintiffs had not identified a standard technical measure that comported with the statute’s definition, the court held that privacy settings do not constitute interference with standard technical measures.³⁶³¹

The court then turned to the requirement that, for the Section 512(c) safe harbor to apply, the infringing material must have been stored at the direction of a user. Ten of the 199 videos in suit had been uploaded by users who were at the time, or later became, Vimeo employees. The court found a material issue of fact concerning the extent to which the ten videos were uploaded by Vimeo employees in their personal capacities as opposed to as agents of Vimeo. Accordingly, a triable issue of fact existed with respect to whether the employees were storing their content as “users” within the meaning of Section 512(c) or as employees

³⁶²⁷ Id. at 513-14.

³⁶²⁸ Id. at 515.

³⁶²⁹ Id.

³⁶³⁰ Id. at 516.

³⁶³¹ Id. at 517.

acting within the scope of their employment. The court therefore denied summary judgment with respect to those ten videos.³⁶³²

The court rejected the plaintiffs' argument that because Vimeo permitted downloading of videos on the web site, it did not provide "storage" within the meaning of Section 512(c). The plaintiffs had provided no case law, and the court was not aware of any, holding or even suggesting that a service provider must be denied DMCA safe harbor protection because it allowed its users to download content. The court also cited the UMG v. Shelter Capital case in which the Ninth Circuit noted that "access-facilitating processes" such as downloading are encompassed in Section 512(c)'s language "by reason of the storage at the direction of a user."³⁶³³

The court then turned to analysis of whether Vimeo had red flag knowledge of infringement that would disqualify it from the safe harbor. The court began its analysis by noting the Second Circuit's ruling in the Viacom v. YouTube case that the difference between actual and red flag knowledge is not between specific and generalized knowledge, but rather between a subjective and an objective standard – actual knowledge turns on whether the service provider subjectively knew of specific infringement, while red flag knowledge turns on whether the service provider was subjectively aware of facts that would have made the specific infringement objectively obvious to a reasonable person. The court found a triable issue of fact as to whether the objective standard of red flag knowledge had been met for 55 of the videos in suit with respect to which Vimeo employees had interacted – the employees provided comments or "liked" 26 of the 55, placed two on channels, "whitelisted" 20 (which precluded other users from flagging the videos for violation of the Terms of Service) and "buried" four (which caused them to no longer appear on Vimeo's home page). The court therefore denied summary judgment with respect to those 55 videos. However, because there was no evidence that Vimeo acquired actual or red flag knowledge as to the 144 videos with which Vimeo employees indisputably did not interact, Vimeo was entitled to summary judgment as to those videos.³⁶³⁴

The court rejected the plaintiffs' argument that Vimeo had been willfully blind to infringement based on an email from a Vimeo employee responding to a user's question asking whether use of copyrighted music in a video was a problem by telling the user that "[w]e allow it, however, if the copyright holder sent us a legal takedown notice, we would have to comply," and another employee responding to a question regarding Vimeo's policy with respect to copyrighted music used as audio for original video content by telling the user, "[d]on't ask, don't tell." Although disconcerting, the court found these examples were insufficient to establish willful blindness because none of them related to the videos in suit. The court held that, just as under Viacom the knowledge prong of Section 512(c) may be met only where the plaintiff is able to prove actual or red flag knowledge as to the specific infringing content at issue in the litigation, so too proof of willful blindness must be tailored to that same infringing content.

³⁶³² Id. at 517-18.

³⁶³³ Id. at 519.

³⁶³⁴ Id. at 520-22.

Here, it was undisputed that none of the examples provided by the plaintiffs, or any other evidence the plaintiffs asserted bore on Vimeo’s willful blindness to infringement, suggested that Vimeo employees were willfully blind to infringing content in any of the specific 199 videos in suit.³⁶³⁵

The court then turned to the right and ability to control prong of Section 512(c), noting that under Viacom, to establish control there must be a showing of “something more” than the ability to remove or block content – specifically, that Vimeo exerted substantial influence on the activities of its users. The plaintiffs argued that Vimeo’s control over user content through its monitoring program constituted “something more.” Members of Vimeo’s “Community Team” enforced the restrictions in the Terms of Service as to the content of uploaded videos, which prohibited unoriginal content as well as commercials, real-estate walkthroughs and “fan vids.” Community Team members utilized approximately 40 software tools to aid their monitoring, including the “Thin Ice” and “Wiretap” tools, which allowed monitoring the activities of specific users suspected of uploading content violative of Vimeo’s policies, the “Sweet Spot” filtering tool, which searched for and listed videos the duration of which Vimeo had determined corresponded to the duration of uploaded television shows or movies, and the “Movie Search” Tool, which ran automated keyword searches for movies currently in theaters. In addition, as to videos that were compliant with Vimeo’s content restrictions, Vimeo staff had significant discretion to manipulate the visibility of such content on the web site, e.g., by promoting a particular video on a popular channel such as the “Staff Picks” channel, “liking” a video and leaving positive comments on a video’s web page. Vimeo staff members could also demote a video through the use of a “burying” tool, the effect of which was that the video did not appear on the “Discover” tab. Finally, the record contained evidence that Vimeo staff communicated directly with some of its users regarding content, at times suggesting to them that it would tolerate the uploading of copyrighted material.³⁶³⁶

The court held that these activities did not constitute “something more” for purposes of the control prong. The court found that the monitoring program did not purport to, and in practice did not, exert substantial influence over the content of the uploaded material, which content Vimeo left in the hands of its users. Unlike the monitoring system in the Cybernet case (discussed in Section III.C.6(b)(1)(iii).d above), Vimeo did not have guidelines that dictated to users the layout, appearance and content of material that could be used on its site. Nor did the ability of Vimeo staff members to demote or promote content constitute control. The court found it difficult to imagine how Vimeo’s staff of 74 people could, through its discretionary and sporadic interactions with video on the web site, exert substantial influence on approximately 12.3 million registered users uploading 43,000 new videos each day. The court therefore found no triable issue as to the exertion of substantial control of user activity.³⁶³⁷

³⁶³⁵ Id. at 523-24.

³⁶³⁶ Id. at 526-29.

³⁶³⁷ Id. at 529-30.

The plaintiffs further argued that Vimeo’s substantial influence over user’s activities was also demonstrated by its inducement of infringement, citing a statement in Viacom that inducement of copyright infringement under Grokster might also rise to the level of control under Section 512(c)(1)(B). The court noted that the Ninth Circuit had expounded upon this inducement theory in its Fung decision (discussed in Section III.C.6(b)(1)(iii).w above), where the Ninth Circuit stated that inducement actions do not categorically remove a service provider from the Section 512(c) safe harbor, although they could supply one essential component of the control prong. The district court noted that the Ninth Circuit’s conclusion was a logical one. Reading the DMCA to mandate that a service provider loses safe harbor protection for conduct identical to that which would subject it to affirmative inducement liability would mean that any attempts by a service provider to seek safe harbor protection upon a finding of affirmative inducement liability would necessarily end before they could even begin. Accordingly, the court stated that, even if the plaintiffs’ inducement argument had some force here, it was skeptical that, under the circumstances of this case, inducement alone could provide an adequate basis for a finding that Vimeo had the right and ability to control.³⁶³⁸

The court did not find persuasive the plaintiffs’ argument that Vimeo induced infringement “by example” – specifically by evidence that some of its employees had created and/or uploaded some of the videos in suit, as well as others with copyrighted or unlicensed music, at least one of which had been the subject of a DMCA takedown notice. The court found such evidence not to rise to the level of that adduced in Grokster, either in quality or in kind. The court found that the relevant standard at issue here – inducement by way of the exertion of substantial influence on the activities of users – could not be met by evidence of “stray” instances of wrongful conduct by Vimeo employees on the web site and/or a generalized effort to promote videos that incorporate music. Accordingly, the court rejected the plaintiffs’ argument that Vimeo employees’ purported “by example” conduct rose to the level of inducement.³⁶³⁹

Nor did Vimeo employees’ communication with, and provision of technical assistance to, Vimeo users constitute inducement of infringement. The court characterized the specific instances of such support cited by the plaintiffs as largely merely offering technical support as to the ordinary use of a service. Although Vimeo offered technical support as to how users could incorporate music into videos, its instructions applied to lawfully and unlawfully incorporated music alike. The court acknowledged that some communications with users may have induced a particular user to infringe in a particular instance. But the relevant standard at issue – inducement by way of exertion of substantial influence on users’ activities – was not met by the limited anecdotal evidence the plaintiffs had provided. The court held that to establish the right and ability to control, there must be a showing that the service provider’s substantial influence

³⁶³⁸ Id. at 530-31.

³⁶³⁹ Id. at 531-33.

over users' activities was significantly more widespread and comprehensive. The court therefore concluded that the plaintiffs' inducement argument failed.³⁶⁴⁰

Finally, the court found that Vimeo had expeditiously removed the videos in suit. On the three occasions, the plaintiffs sent Vimeo a takedown notice and Vimeo removed the videos identified in the notices. One letter from one of the plaintiffs identified approximately 170 videos on the web site that infringed, and Vimeo removed the videos within approximately three and one-half weeks. The court found that, given the number of infringing videos at issue, the three and one-half week period it took Vimeo to comply with the notice constituted expeditious removal. Vimeo had responded to all other takedown notices from the plaintiffs within the same day.

In sum, the court ruled that a triable issue existed as to whether the ten employee-uploaded videos were "stored at the direction of a user" and as to whether Vimeo had knowledge or awareness of infringing content in the 55 of the 199 videos in suit with which Vimeo employees interacted. Accordingly, Vimeo's motion for summary judgment seeking safe harbor protection was granted as to the remaining 144 videos in suit, save for those videos in suit containing infringed upon material recorded before February 15, 1972.³⁶⁴¹ The plaintiffs' cross motion for partial summary judgment was granted solely as to videos in suit containing infringing musical recordings which were recorded prior to February 15, 1972.³⁶⁴²

The defendants filed a motion for reconsideration, asking the court to reconsider its decision with respect to 35 of the 55 videos with which Vimeo employees interacted. The court, in a subsequent opinion, granted summary judgment to Vimeo with respect to 15 of the 35 videos because, upon further review of the record, the court agreed with Vimeo that no evidence showed that Vimeo employees actually viewed the content of those videos.³⁶⁴³ With respect to the remaining 20 of the videos, the defendants argued that the infringing nature of the videos was not obvious because each contained some original elements and their creators thus had at least a colorable defense that they made fair use of the copyrighted material, and the videos could therefore not provide red flag knowledge to Vimeo. The court reviewed the remaining 20 videos and determined that, with respect to 18 of them, a reasonable juror could (but need not) find that the infringing activity in each video was objectively obvious to a reasonable person because the videos played virtually all of the copyrighted song, most of them displayed both the artist and song title, and the songs were an integral part of the videos, with the length of the video corresponding to the length of the song. But the court determined that the defendants were entitled to summary judgment on the other two videos because evidence of infringement was not objectively obvious in them. In each of them, the copyrighted songs

³⁶⁴⁰ Id. at 533-35.

³⁶⁴¹ The plaintiffs argued that the DMCA safe harbors do not extend to recordings first fixed before February 15, 1972 and the court agreed for the reasons discussed in Section III.C.6(b)(8) below. See id. at 536-37.

³⁶⁴² Id. at 537.

³⁶⁴³ Capitol Records, LLC v. Vimeo, 972 F. Supp. 2d 537, 543-45 (S.D.N.Y. 2013), aff'd in part & vacated and remanded in part, 826 F.3d 78 (2d Cir. 2016).

played for only a short time in the background (less than a minute) in the middle of the video, and neither the name of the song nor the artist was displayed anywhere in the video or on the web page through which users could view the video.³⁶⁴⁴

In addition, the court granted Vimeo's request to certify for interlocutory appeal to the Second Circuit the following two questions:

(1) Whether the DMCA's safe-harbor provisions are applicable to sound recordings fixed prior to February 15, 1972 (the Second Circuit's rulings on this issue are discussed in Section III.C.6(b)(8)(i) below); and

(2) Whether, under *Viacom Int'l. Inc. v. YouTube, Inc.*, a service provider's viewing of a user-generated video containing all or virtually all of a recognizable, copyrighted song may establish "facts or circumstances" giving rise to "red flag" knowledge of infringement.³⁶⁴⁵

The Second Circuit's Decision

On interlocutory appeal of the second issue, the Second Circuit vacated the district court's rulings in part, affirmed in part, and remanded.³⁶⁴⁶ The Second Circuit began its analysis by noting that the district court's formulation of the certified question suggested that the court based its denial of Vimeo's motion for summary judgment on the presence of the facts specified in the question. The Second Circuit concluded that the plaintiffs' establishment of those facts was insufficient to prove red flag knowledge.³⁶⁴⁷

The court recited its holding in *Viacom* that the difference between actual and red flag knowledge is not between specific and generalized knowledge, but instead between a subjective and an objective standard. In other words, the actual knowledge provision turns on whether the provider actually or subjectively knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement objectively obvious to a reasonable person. The court elaborated that the hypothetical "reasonable person" to whom infringement must be obvious is an ordinary person, not endowed with specialized knowledge or expertise concerning music or the laws of copyright.³⁶⁴⁸

In view of Section 512(m)'s provision that the service provider is under no duty to affirmatively seek indications of infringement, the court concluded the mere fact that an

³⁶⁴⁴ *Id.* at 546-47. The court also granted the plaintiffs leave to file an amended complaint to add 1476 new instances of infringement. *Id.* at 549-50.

³⁶⁴⁵ *Id.* at 556.

³⁶⁴⁶ *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78 (2d Cir. 2016).

³⁶⁴⁷ *Id.* at 93.

³⁶⁴⁸ *Id.* at 93-94.

employee of the service provider has viewed a video posted by a user (absent specific information regarding how much of the video the employee saw or the reason for which it was viewed), and that the video contained all or nearly all of a copyrighted song that is recognizable, would be insufficient to make infringement obvious to an ordinary reasonable person, who is not an expert in music or the law of copyright. Because the district court's denial of Vimeo's motion for summary judgment and concomitant certification of the question suggested that the district court believed the evidence described in the question, without more, could render the service provider ineligible for the safe harbor, and relied on this proposition to deny summary judgment in every instance in which there was evidence that an employee of Vimeo had seen at least a portion of a video that contained substantially all of a recognizable copyrighted song, the court concluded that it must vacate the district court's ruling on the question and remand for reconsideration in light of its further discussion of the standard for red flag knowledge.³⁶⁴⁹

The court then elaborated on the applicable burdens of proof regarding a defendant's eligibility for the safe harbor, particularly with respect to the issue of red flag knowledge. The court stated that a service provider's entitlement to the safe harbor is properly seen as an affirmative defense, and therefore must be raised by the defendant. The defendant bears the burden of raising entitlement to the safe harbor and of demonstrating that it has the status of service provider, as defined, and has taken the steps necessary for eligibility. On the other hand, on the question whether the service provider should be disqualified based on the copyright owner's accusations of misconduct – i.e., by reason of the service provider's failure to act as the statute requires after receiving the copyright owner's notification or otherwise acquiring actual or red flag knowledge – the burden of proof shifts to the plaintiff.³⁶⁵⁰

The court then cited and agreed with Prof. Nimmer's treatise explaining the shifting allocations of burdens of proof as to the service provider's entitlement to the Section 512(c) safe harbor. Following Nimmer's analysis, a defendant bears the burden, in the first instance, to show entitlement to the safe harbor defense by demonstrating its status as a service provider that stores users' material on its system, that the allegedly infringing matter was placed on its system by a user, and that it has performed precautionary, protective tasks required by Section 512 as conditions of eligibility, including that it adopted and reasonably implemented a policy designed to exclude users who repeatedly infringe, that it designated an agent for receipt of notices of infringement, and that it accommodates standard technical measures used by copyright owners to detect infringements. On the issue of disqualifying knowledge, however, the burden falls on the copyright owner to demonstrate that the service provider acquired knowledge of the infringement, or of facts and circumstances from which infringing activity was obvious, and failed to promptly take down the infringing matter, thus forfeiting its right to the safe harbor. The plaintiff is entitled to take discovery of the service provider to enable it to make this showing.³⁶⁵¹

³⁶⁴⁹ *Id.* at 94.

³⁶⁵⁰ *Id.*

³⁶⁵¹ *Id.* at 94-95.

The court ruled that a copyright owner's mere showing that a video posted by a user on the service provider's site includes substantially all of a recording of recognizable copyrighted music, and that an employee of the service provider saw at least some part of the user's material, is insufficient for many reasons to sustain the copyright owner's burden of proving that the service provider had either actual or red flag knowledge of the infringement. First, the employee's viewing might have been brief. Second, there may be many different business purposes for which the employee might have viewed the video, such as applying technical elements of computer expertise, classification of subject matter, sampling to detect inappropriate obscenity or bigotry, or other objectives having nothing to do with recognition of infringing music in the soundtrack. The fact that music is recognizable or even famous is insufficient to demonstrate that the music was in fact recognized by a hypothetical ordinary individual who has no specialized knowledge of the field of music. Third, employees of service providers cannot be assumed to have expertise in the laws of copyright. Even assuming awareness that a user posting contains copyrighted music, the service provider's employee cannot be expected to know how to distinguish between infringements and, for example, parodies that may qualify as fair use. Nor can every employee of a service provider be automatically expected to know how likely or unlikely it may be that the user who posted the material had authorization to use the copyrighted music. Even an employee who was a copyright expert cannot be expected to know when use of a copyrighted song has been licensed.³⁶⁵²

The plaintiffs argued that the court's understanding of red flag knowledge reduced it to a very small category. The court replied that, assuming this is so, it is of no significance. The fact that Congress was unwilling to extend the safe harbor to circumstances where the service provider did not subjectively know that the posted material infringed, but did know facts that make infringement objectively obvious, did not compel the conclusion that Congress expected this extension to cover a large number of instances. That was especially so in view of the fact that the purpose of Section 512(c) was to give service providers immunity, in exchange for augmenting the arsenal of copyright owners by creating the notice-and-takedown mechanism.³⁶⁵³

The court concluded that, as to the red flag knowledge issue, Vimeo was entitled to summary judgment on those videos as to which the plaintiffs had shown no more than that some employee of Vimeo had some contact with those videos and they played all, or nearly all, of a recognizable song, unless the plaintiffs could point to evidence sufficient to carry their burden of proving that Vimeo personnel either knew the video was infringing or knew facts making that conclusion obvious to an ordinary person who had no specialized knowledge of music or the law of copyright.³⁶⁵⁴

³⁶⁵² Id. at 96-97.

³⁶⁵³ Id. at 97.

³⁶⁵⁴ Id. at 97-98.

Lastly, the court turned to the plaintiffs' contention that the district court, in rejecting their claim of willful blindness, misapplied the teachings of Viacom. The plaintiffs made three arguments. First, based on evidence that Vimeo monitored videos for infringement of visual content but not for infringement of audio content, they argued that they had demonstrated willful blindness to infringement of music. Second, they argued that Vimeo's awareness of facts suggesting a likelihood of infringement gave rise to a duty to investigate further, and that Vimeo's failure to do so showed willful blindness. Third, they argued that, having encouraged users to post infringing matter, Vimeo could not then close its eyes to the resulting infringements without liability.³⁶⁵⁵

The court rejected these arguments. With respect to the first argument, the court noted Viacom made clear that Section 512(m) relieves the service provider of an obligation to monitor for infringements posted by users on its web site. The court saw no reason why Vimeo's voluntary undertaking to monitor videos for infringement of visual material should deprive it of the statutory privilege not to monitor for infringement of music. With respect to the second argument, the court saw no reason to construe the statute as vitiating the protection of Section 512(m) and requiring investigation merely because the service provider learned facts raising a *suspicion* of infringement (as opposed to facts making infringement *obvious*). If providers were compelled constantly to take stock of all information their employees might have acquired that might suggest the presence of infringements in user postings, and to undertake monitoring investigations whenever some level of suspicion was surpassed, those obligations would largely undo the value of Section 512(m).³⁶⁵⁶

With respect to the plaintiffs' third argument, the court noted that, although it might fare better in theory, it was not supported by the facts of this case. Viacom made clear that actual and red flag knowledge under the DMCA ordinarily must relate to specific infringing material and that, because willful blindness is a proxy for knowledge, it too must relate to specific infringements. The plaintiffs argued that, notwithstanding the formulation in Viacom, a service provider cannot adopt a general policy of urging or encouraging users to post infringing material and then escape liability by hiding behind a disingenuous claim of ignorance of the users' infringements.³⁶⁵⁷

The court found that it need not decide whether the plaintiffs' proposed gloss on Viacom was correct as a matter of law. The evidence cited to the court by the plaintiffs, consisting of a handful of sporadic instances among millions of posted videos in which Vimeo employees inappropriately encouraged users to post videos that infringed music could not support a finding of the sort of generalized encouragement of infringement supposed the plaintiffs' legal theory. It therefore could not suffice to justify stripping Vimeo completely of the protection of Section 512(m). Moreover, because that evidence was not shown to relate to any of the videos at issue in the suit, it was insufficient to justify a finding of red flag knowledge under the principles of

³⁶⁵⁵ Id. at 98.

³⁶⁵⁶ Id. at 98.

³⁶⁵⁷ Id. at 98-99.

Viacom as to those specific videos. Thus, notwithstanding a few unrelated instances in which its employees improperly encouraged specific infringements, Vimeo could still assert the protection of Section 512(m) for the present suit, and claim the benefit of the safe harbor, in the absence of a showing by the plaintiffs of facts sufficient to demonstrate that Vimeo, having actual or red flag knowledge of infringement in the videos in suit failed to promptly take them down.³⁶⁵⁸

In sum, for the reasons given, the court vacated the district court's denial of Vimeo's motion for summary judgment on the videos with respect to which it had found red flag knowledge and remanded for further proceedings, and affirmed the district court's ruling in Vimeo's favor as to the plaintiffs' reliance on the doctrine of willful blindness.³⁶⁵⁹

The District Court's Decision on Remand

On remand, the court noted that under the Second Circuit's decision, the burden was on the plaintiffs to show that the Vimeo employee who interacted with a specific video recognized the music contained in the video and knew of facts sufficient to determine that use of the copyrighted music was neither authorized nor fair. The court found that the plaintiffs had not made a sufficient showing. The evidence demonstrated only that some employees at the company were broadly familiar with the concept of copyright and there was some general awareness within the company that copyright infringement was occurring on Vimeo.com, but the evidence shed no light on whether the employees who screened the videos at issue possessed particularized knowledge of copyright law (as some Vimeo executives may have had). Nor had plaintiffs adduced any evidence establishing that Vimeo knew that major music labels generally had not authorized their music to be distributed in the format available on Vimeo. And even if Vimeo did adopt a cavalier approach toward copyright infringement, that would not disqualify it from the safe harbor, because it would not demonstrate that Vimeo failed to act in the face of specific, objectively obvious instances of infringement. Although some of the plaintiffs' evidence permitted an inference that some Vimeo employees may have been broadly familiar with concepts such as fair use, it did not, on its own, permit the court to infer that this knowledge armed employees with the ability to distinguish infringements from authorized or fair use with respect to any of the videos at issue.³⁶⁶⁰

Nor was the plaintiffs' evidence of employee interactions with the videos sufficient, including tagging the video with music credits, liking and commenting on videos, whitelisting or burying videos, placing videos on a Vimeo-moderated channel, and inducing the creation of certain types of videos. Proof that the employees identified the presence of copyrighted material was a necessary but insufficient condition of red flag knowledge. These modes of interaction with infringing videos said nothing about the employee's knowledge as to whether the use of such music was authorized or fair. The court also rejected the plaintiffs' argument that their cease and desist letters and complaints imparted red flag knowledge with respect to a

³⁶⁵⁸ Id. at 99.

³⁶⁵⁹ Id.

³⁶⁶⁰ Capitol Records, LLC v. Vimeo, LLC, 2021 U.S. Dist. LEXIS 101663 at *13-23 (S.D.N.Y. May 28, 2021).

subset of the videos at issue. The court observed that under this view of DMCA liability, once the plaintiffs had identified a particular artist in a complaint as an artist whose music appeared unlawfully on Vimeo's web site, red flag knowledge would be imputed to Vimeo with respect to all subsequently uploaded, user-generated videos containing music by that artist. The court ruled that contention misconstrued the concept of red flag knowledge – the fact that an artist's copyright was previously infringed on Vimeo would not suffice to indicate to an employee whether use of that artist's work in a subsequent video was authorized. Absent proof that Vimeo employees had "categorical knowledge" about the licensing practices of particular artists, the timing of employee interactions with the videos at issue could not create a triable issue of fact on red flag knowledge. Accordingly, the defendants were entitled to summary judgment on the safe harbor as to all videos uploaded by users unaffiliated with Vimeo.³⁶⁶¹

The court, however, denied summary judgement to both the plaintiffs and the defendants as to videos uploaded or partially created by Vimeo employees because of fact questions concerning whether they stored content as "users" or as employees acting within their scope of employment.³⁶⁶²

aa. Perfect 10 v. Giganews

The facts of this case are set forth in Section III.C.2(n) above. After the court's preliminary rulings on Giganews' motions to dismiss the claims of direct, contributory and vicarious liability (see Sections II.A.4(v) and III.C.2(n) above), Perfect 10 sought summary judgment on the defendants' assertions of the Section 512(c) safe harbor. At issue were whether five notices Perfect 10 sent to Giganews met the requirements of Section 512(c)(3)(A), whether Giganews had reasonably implemented a repeat infringer termination policy, and whether Giganews satisfied other requirements for safe harbor protection.³⁶⁶³

Turning first to the adequacy of Giganews' repeat infringer policy, the court noted that Giganews had a "two-strike" policy – upon learning that a user had posted an infringing message, Giganews froze the user's account and provided a warning that another infringement would result in termination of the account. If the user responded that he or she would not post any additional infringing material, the account was unfrozen. If Giganews was informed that the user had posted any additional infringing material, the user's account would be terminated. The court concluded that this was sufficient to establish that Giganews had established a repeat infringer policy. It then turned to Perfect 10's challenge concerning whether Giganews had reasonably implemented its policy.³⁶⁶⁴

Perfect 10 argued that Giganews was required to remove all of a repeat infringer's content, not just the content a copyright holder had specifically identified as infringing. The

³⁶⁶¹ Id. at *23-42.

³⁶⁶² Id. at *42-44.

³⁶⁶³ Perfect 10, Inc. v. Giganews, Inc., 993 F. Supp. 2d 1192, 1194 (C.D. Cal. 2014).

³⁶⁶⁴ Id. at 1197.

court rejected this argument on the ground that Section 512(i)(a)(A) refers to termination of subscribers and account holders, not the deletion of messages. In addition, Perfect 10's reading would require a service provider to take down all of a user's messages, not just the infringing ones, which would not serve any purpose of preventing infringement. The court therefore rejected Perfect 10's argument. Perfect 10 also argued that the fact that Giganews had terminated only 46 repeat infringers since 2008 despite removing more than 531 million infringing messages over the past year demonstrated that Giganews did not properly implement its policy. The court rejected this argument, noting that the inference Perfect 10 sought to draw from such facts was not compelled and therefore was an inadequate basis for summary judgment.³⁶⁶⁵

Next Perfect 10 argued that the fact that Giganews did not know the identity of all users whose messages resided on its servers demonstrated that Giganews' policy was inadequate, because if Giganews could not identify a user, it could not reasonably implement a repeat infringer termination policy. The court rejected this argument. Because all USENET service providers encrypt the data that identifies the user who posted a message, only the USENET service provider with whom an account was registered could decrypt the "X-trace" field in the message header that stored the user's name. Many of the messages hosted on Giganews servers were posted through accounts registered with other USENET providers. Because Giganews could not decrypt the X-trace field on such messages, it could not link such messages to any specific users, and thus could not apply its repeat infringer termination policy to such users. These facts therefore precluded summary adjudication that Giganews did not reasonably implement its repeat infringer termination policy.³⁶⁶⁶

The court next ruled that Perfect 10 had not established that its five takedown notices at issue complied with Section 512(c)(3)(A). The notices at issue instructed Giganews to use certain newsreaders to conduct searches of specific names within certain newsgroups, and then informed Giganews that all of the messages yielded by those searches on a certain date contained infringing material. Along with verbose instructions for performing the searches, the notices included pages of thumbnail images of the infringing materials and/or screen shots of the newsreader interface reflecting the search results. Giganews contended that the notices were inadequate because they failed to include the "Message-ID" (a unique string of letters and numbers assigned to every USENET message) for each infringing message. The court was not convinced that Perfect 10's approach of pointing to the results of a search performed on a specific date at a specific time on a specific newsreader, and attaching thumbnail images and screen shots, amounted to adequate identification of the infringing material as required by Section 512(c)(3)(A). First, the method pointed only to a list of search results, not to any material in particular. Second, because material accessible through the USENET is in a constant state of flux, there was no certainty that any particular search would yield the exact same results at different times. Under the plaintiff's method of identifying infringing material, Giganews would be required to compare its search results to Perfect 10's search results to see if they were

³⁶⁶⁵ Id. at 1197-98.

³⁶⁶⁶ Id.

the same, *and* to distinguish between material that infringed Perfect 10's copyright and material that did not. The court therefore concluded that it could not resolve summary adjudication in Perfect 10's favor that such methodology constituted adequate identification of infringing material.³⁶⁶⁷

In addition, the court noted that under Section 512(c)(3)(A), notices must provide information reasonably sufficient to permit the service provider to remove the offending material expeditiously. Giganews argued that only a Message-ID was adequate for the purpose of removal. In response, Perfect 10 pointed to several other variables in message headers that could be used in combination to locate a message. The court rejected this argument, noting that a Message-ID sufficed to locate a message, and adding more variables to the location process only served to complicate it. The parties submitted evidence that Message-IDs could be extracted either manually or by a computer program written to extract them automatically. In addition, third party service providers were available who could prepare DMCA notices with Message-IDs. Based on this evidence, the court noted that the crux of the parties' dispute was who must bear the burden of extracting the Message-IDs associated with the infringing messages. Giganews argued that if it had to extract Message-IDs for the hundreds of millions of messages identified in DMCA notices it had received, it would not be able to function. Perfect 10 countered that Giganews did extract Message-IDs for infringing messages reflected in two of its notices and argued that fact demonstrated that all notices lacking Message-IDs were sufficient to allow Giganews to locate the messages. Based on this evidence, the court concluded that triable issues precluded summary adjudication of the issue in Perfect 10's favor.³⁶⁶⁸

Finally, Perfect 10 contended that Giganews could not qualify for the Section 512(c) safe harbor because the infringing messages were not being stored at the direction of users, in view of the fact that Giganews copied infringing messages to its servers without the intervention of third party users and stored them as long it wanted. The court rejected this argument. Because USENET messages are propagated automatically once they are posted by a third party user, the court found such propagation was arguably "at the direction of" a user. The court therefore concluded that the question of whether Giganews was eligible for the Section 512(c) safe harbor could not be summarily adjudicated in Perfect 10's favor.³⁶⁶⁹

Ultimately, Giganews did not need to rely on the DMCA safe harbor, as it was able to obtain summary judgment in its favor based on Perfect 10's failure to prove the required elements of direct, contributory and vicarious liability. See Sections II.A.4(v) and III.C.2(n) above.

bb. Rosen v. Global Net Access

³⁶⁶⁷ Id. at 1199-1200.

³⁶⁶⁸ Id. at 1200-01.

³⁶⁶⁹ Id. at 1202.

The court's rulings with respect to why Global Net Access was not entitled to the Section 512(c) safe harbor are discussed in Section III.C.2(p) above.

cc. Mavrix Photographs v. LiveJournal

The District Court's Decision

In Mavrix Photographs LLC v. LiveJournal, Inc.,³⁶⁷⁰ LiveJournal operated a web-based social media platform that allowed users to create personalized online "journals." Users could post content to their personal journals or to communities they joined. Certain communities were moderated, and for those communities, when a user submitted a post, it was automatically uploaded onto LiveJournal's servers and placed in a queue. Any moderator signed in at the time could reject the post or approve it, at which point it became visible to the community. The plaintiff Mavrix owned the copyrights in seven photos that were uploaded without authorization by users to a blogging community. LiveJournal asserted the Section 512(c) safe harbor as a defense.³⁶⁷¹

LiveJournal's Terms of Service expressly prohibited the posting of content that infringed any copyright of a third party. LiveJournal had in place a policy to terminate the accounts of users who were repeat copyright infringers, even going as far as to block their IP addresses so they could not register a new LiveJournal account. LiveJournal provided a form, contact information, and a designated agent for submission of notices of copyright infringement. Upon receipt of a DMCA-compliant take-down notice, LiveJournal promptly disabled the material claimed to be infringing, typically within 24 hours and no longer than three days pursuant to its internal policy. Although Mavrix made no attempt to send LiveJournal a DMCA notice or otherwise notify LiveJournal of the seven allegedly infringing photos before filing suit, upon receipt of Mavrix's complaint, LiveJournal disabled access to the posts containing the alleged infringement. Two of the posters were repeat offenders under LiveJournal's copyright abuse policy, so LiveJournal terminated their accounts. Mavrix did not challenge LiveJournal's satisfaction of the safe harbor predicate conditions of having a designated agent and having adopted and reasonably implemented a repeat infringer termination policy.³⁶⁷²

Instead, Mavrix contended that LiveJournal was not eligible for the Section 512(c) safe harbor because the "at the direction of the user" language in Section 512(c) confines the safe harbor to situations such as where infringing material has been emailed to the editor of a newspaper and resides on the newspaper's servers, but is never made accessible to the public. The court rejected this argument, noting that under Ninth Circuit authority the safe harbor is clearly meant to cover more than mere electronic storage lockers in which material is not made available to the public. And it was undisputed that third party users selected the content for the

³⁶⁷⁰ 2014 U.S. Dist. LEXIS 160324 (C.D. Cal. Sept. 19, 2014), rev'd and remanded, 2017 U.S. App. LEXIS 16624 (9th Cir. Apr. 7, 2017).

³⁶⁷¹ Id. at *2-5.

³⁶⁷² Id. at *5-8 & *13 n.6.

seven posts in question, created the posts, and uploaded the posts to LiveJournal's services. That all posts had to be approved by a moderator before becoming visible on the site did not disqualify LiveJournal under the broad statutory language of the safe harbor for "infringement ... by reason of the storage at the direction of the user."³⁶⁷³

Turning to the other requirements of the safe harbor, the court noted that Mavrix had not given LiveJournal actual notice of the infringements before filing the complaint. The court rejected Mavrix's argument that LiveJournal could have "red flag" knowledge based solely on the fact that the photos were allegedly of the type of material frequently shot by professional paparazzi photographers. Indeed, the court noted that the nature of the photos at issue suggested just the opposite, because the photos were candid images of celebrities in public settings, un-posed, mostly taken from the back or the side without the subject looking at the camera. With respect to the right and ability to control the infringing activity, the court noted that the pertinent inquiry was not whether LiveJournal had the right and ability to control its system, but rather whether it had the right and ability to control the infringing activity. The court ruled that it did not, because the undisputed facts showed that users of the LiveJournal service, not LiveJournal, selected the content to be posted, put that content together into a post, and uploaded the post to LiveJournal's service. LiveJournal did not solicit any specific infringing material from its users or edit the content of its users' posts. Nor did it have the ability to do so.³⁶⁷⁴

Finally, the court ruled that Mavrix was not entitled to any of the narrow forms of injunctive relief permitted under the statute, because it was undisputed that LiveJournal had already disabled access to the infringing posts and had terminated the two users who qualified as repeat offenders under its policy. Accordingly, injunctive relief under Section 512(j)(1)(A)(i) would be moot. Mavrix asserted that it might be eligible for relief under Section 512(j)(1)(A)(iii) allowing for "other relief" as the court might consider necessary to prevent or restrain infringement at a particular online location. The court rejected this as well, noting that the undisputed facts showed that the only technical measure in LiveJournal's service that could be used to prevent users from uploading Mavrix's photos in the future was its "anti-spam" system, which could block users from uploading posts with specific keywords. The court noted it was undisputed that LiveJournal had already employed that measure to block posts with the keyword "mavrix-online.com." Accordingly, the court granted summary judgment to LiveJournal that it was entitled to the Section 512(c) safe harbor for the seven allegedly infringing posts.³⁶⁷⁵

The Ninth Circuit's Decision

On appeal, the Ninth Circuit reversed and remanded. The court cast the key issue for decision as whether the common law of agency applied to LiveJournal's safe harbor defense.

³⁶⁷³ Id. at *14-15.

³⁶⁷⁴ Id. at *18-19, *22.

³⁶⁷⁵ Id. at *27-29.

Noting that the district court had ruled it did not, the Ninth Circuit disagreed and concluded that it did.³⁶⁷⁶

The court began its analysis by noting that LiveJournal was required to make a threshold showing that Mavrix's photographs were stored at the direction of the user:

"Storage," in this context, has a unique meaning. Congress explained that "[e]xamples of such storage include providing server space for a user's web site, for a chatroom, or other forum in which material may be posted at the direction of users." S. Rep. 105-190, at 43 (1998). We have held that storage "encompasses the access-facilitating processes" in addition to storage itself. *Shelter Capital*, 718 F.3d at 1016 (rejecting a claim that the safe harbor addresses mere storage lockers). We reasoned that rather than requiring "that the infringing conduct *be* storage," the statutory language allows for infringement "*by reason of the storage* at the direction of a user." *Id.* (emphasis added).³⁶⁷⁷

The court noted further that the Section 512(c) safe harbor focuses on the service provider's role in making material stored by a user publicly accessible on its site.³⁶⁷⁸ "Contrary to the district court's view, public accessibility is the critical inquiry. In the context of this case, that inquiry turns on the role of the moderators in screening and posting users' submissions and whether their acts may be attributed to LiveJournal."³⁶⁷⁹ Noting that the Ninth Circuit had previously applied the common law of vicarious liability in analyzing the DMCA's safe harbors, as well as a service provider's intent to infringe under the DMCA, the court found little difficulty holding that common law agency principles should apply to the analysis of whether a service provider like LiveJournal is liable for the acts of its moderators.³⁶⁸⁰ The court noted that such a ruling might be in conflict with the Tenth Circuit's decision in BWP Media USA, Inc. v. Clarity Dig. Grp., LLC, in which the Tenth Circuit held that the service provider's contractors were "users" rather than agents under the DMCA, and that even if the contractors were agents or employees, they could still be users.³⁶⁸¹ The Ninth Circuit stated, "To the extent that *BWP*'s holding contradicts our case law that common law principles of agency apply to the DMCA such that a service provider is liable for the acts of its agents, including its employees, we reject it."³⁶⁸²

The court concluded that there were genuine issues of material fact as to whether LiveJournal's moderators were its agents. First, the court noted that LiveJournal's moderators performed a vital function in its business model. There was evidence that LiveJournal gave moderators express directions about their screening functions, including criteria for accepting or

³⁶⁷⁶ 873 F.3d 1045, 1049 (9th Cir. 2017) (amended opinion) (original opinion at 853 F.3d 1020 (9th Cir. 2017)).

³⁶⁷⁷ *Id.* at 1052-53.

³⁶⁷⁸ *Id.* at 1053.

³⁶⁷⁹ *Id.*

³⁶⁸⁰ *Id.* at 1053.

³⁶⁸¹ 820 F.3d 1175, 1180-81 (10th Cir. 2016).

³⁶⁸² Mavrix, 873 F.3d at 1053 n.8.

rejecting posts. Unlike other sites where users could independently post content, LiveJournal relied on moderators as an integral part of its screening and posting business model. LiveJournal also provided three different levels of authority: moderators reviewed posts to ensure they contained celebrity gossip and not pornography or harassment, maintainers deleted posts and could remove moderators, and owners could remove maintainers. Genuine issues of material fact therefore existed regarding whether the moderators had actual authority.³⁶⁸³

Second, there was evidence that LiveJournal users may have reasonably believed that the moderators had authority to act for LiveJournal. For example, one user relied on the moderators' approval as a manifestation that the post complied with copyright law, and the user appeared to believe the moderators acted on behalf of LiveJournal. Accordingly, genuine issues of material fact existed regarding whether moderators had apparent authority.³⁶⁸⁴

Third, there were genuine issues of material fact regarding the level of control LiveJournal exercised over moderators. Evidence presented by Mavrix showed that LiveJournal's head moderator, Brendan Delzer, who was a full time employee acting as the community's full time "primary leader," gave other moderators substantive supervision and selected and removed them on the basis of their performance, thus demonstrating control. Delzer also exercised control over the moderators' work schedules. On the other hand, moderators were free to leave and go and volunteer their time in any way they saw fit. They could reject submissions for reasons other than those provided by the rules, which called into question the level of control that LiveJournal exerted over their conduct.³⁶⁸⁵

The court then turned to a related issue that the fact finder must resolve on remand in the event there was a finding that the moderators were agents of LiveJournal – specifically, whether Mavrix's photographs were indeed stored at the direction of the users in view of the moderators' role in screening and posting the photographs. The court noted that infringing material is stored at the direction of the user if the service provider played no role in making that infringing material accessible on its site or if the service provider carried out only activities that were narrowly directed toward enhancing the accessibility of the posts. Accessibility-enhancing activities include automatic processes, for example, to reformat posts or perform some technological change. Some manual service provider activities that screen for infringement or other harmful material like pornography can also be accessibility-enhancing activities.³⁶⁸⁶ The court also noted that the Second Circuit had found it a close call and remanded when YouTube manually selected videos for front page syndication on the basis of substance, and on remand the district court in that case held only those processes without manual intervention satisfied

³⁶⁸³ *Id.* at 1054-55.

³⁶⁸⁴ *Id.* at 1055.

³⁶⁸⁵ *Id.* at 1050, 1055-56.

³⁶⁸⁶ *Id.* at 1056.

the Section 512(c) safe harbor.³⁶⁸⁷ Accordingly, the Ninth Circuit seems to have signaled that the scope of accessibility-enhancing activities that will not remove a service provider from the Section 512(c) safe harbor may be rather circumscribed: “The question for the fact finder is whether the moderators’ acts were merely accessibility-enhancing activities or whether instead their extensive, manual, and substantive activities went beyond the automatic and limited manual activities we have approved as accessibility-enhancing.”³⁶⁸⁸

The Ninth Circuit then turned to the question whether LiveJournal had actual or red flag knowledge of the infringements. The court noted that both actual and red flag knowledge refer to knowledge of the *specific* infringements. On remand, the fact finder must first determine whether LiveJournal had actual knowledge of the infringements, and to fully assess actual knowledge, the fact finder should also assess a service provider’s subject knowledge of the infringing nature of the posts. Here, Mavrix had not had the opportunity to depose the moderators to determine whether the moderators (if found to be agents) had actual knowledge of the infringing nature of the posts.³⁶⁸⁹

If the moderators lacked actual knowledge, then the fact finder must assess whether LiveJournal had red flag knowledge. The infringement must be immediately apparent to a non-expert. The court noted that some of the photographs at issue in the case contained either a generic watermark or a watermark containing Mavrix’s web site “Mavrixonline.com.” Thus, to determine whether LiveJournal had red flag knowledge, the fact finder should on remand assess if it would be objectively obvious to a reasonable person that material bearing a generic watermark or a watermark referring to a service provider’s web site was infringing.³⁶⁹⁰

Finally, if the fact finder determined that the photographs were stored at the direction of the user and that LiveJournal lacked knowledge of the infringements, then the fact finder should determine whether LiveJournal showed that it did not financially benefit from infringements that it had the right and ability to control. The fact finder should consider the service provider’s procedures that existed at the time of the infringements when assessing the service provider’s right and ability to control the infringements.³⁶⁹¹ In an important elaboration, the Ninth Circuit stated, “The fact finder should consider the service provider’s *general practices*, not its conduct with respect to the specific infringements.”³⁶⁹² The court noted that right and ability to control

³⁶⁸⁷ *Id.* at 1056 n.12 (citing *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 40 (2d Cir. 2012) and *Viacom Int’l v. YouTube, Inc.*, 940 F. Supp. 2d 110, 123 (S.D.N.Y. 2013)).

³⁶⁸⁸ *Mavrix*, 873 F.3d at 1056.

³⁶⁸⁹ *Id.* at 1057.

³⁶⁹⁰ *Id.* at 1057-58.

³⁶⁹¹ *Id.* at 1058.

³⁶⁹² *Id.* (emphasis added). Contrast this focus on the general practices of the service provider with the Ninth Circuit’s narrower rule that, to establish common law vicarious liability, a plaintiff must demonstrate a causal link between the *infringing activities in the case at hand* and a financial benefit to the defendant service provider from those infringing activities. *Perfect 10, Inc. v. Giganews, Inc.*, 847 F.3d 657, 673 (9th Cir. 2017). See discussion of the *Giganews* case in Section III.C.2(n) above.

involves something more than the ability to remove or block access to materials posted on the service provider's web site, such as the exertion of high levels of control over activities of users. The right and ability to control may also be shown by intentional inducement of infringement, although inducement was not at issue in this particular case. The court noted that LiveJournal's rules instructed users on the substance and infringement of their posts. The moderators screened for content and other guidelines such as infringement. Nearly two-thirds of submitted posts were rejected, including on substantive grounds. The court then stated that in determining whether LiveJournal had the right and ability to control infringements, the fact finder must assess whether LiveJournal's extensive review process constituted high levels of control to show "something more."³⁶⁹³

With respect to the financial benefit issue, the court noted that LiveJournal derived revenue from advertising based on the number of views the web site received. Mavrix presented evidence showing that approximately 84% of posts on the site contained infringing material, although LiveJournal contested the validity of the evidence. The court noted that the fact finder should determine on remand whether LiveJournal financially benefitted from infringement that it had the right and ability to control.³⁶⁹⁴

Under the Ninth Circuit's decision in Mavrix, a service provider may lose the safe harbor protection if its efforts to curate materials available on its platform are substantive and sufficiently extensive to constitute more than "accessibility-enhancing activities." The decision may therefore incentivize service providers seeking to avail themselves of the Section 512(c) safe harbor to exercise less oversight of materials that users submit for posting, which in turn may cause detriment to the service provider's business model.

dd. Rosen v. eBay

In Rosen v. eBay, Inc.,³⁶⁹⁵ the plaintiff Rosen was the owner of copyrights in several photographs. He sought to hold eBay directly³⁶⁹⁶ and secondarily liable for copyright infringement based on the offering for sale of unauthorized copies of his photographs through third party sellers on the eBay marketplace. eBay filed a motion for summary judgment based on the Section 512(c) safe harbor. Rosen argued that eBay was ineligible for the safe harbor on a number of grounds. First, eBay submitted declarations stating that it had implemented a policy for the termination of repeat infringers by October 2000 and had since "suspended" repeat

³⁶⁹³ Id. at 1058-59. The court deleted from the amended opinion the observation in its original opinion that LiveJournal maintained a list of sources that had complained about infringement from which users should not submit posts, and went so far as to use a tool to automatically block any posts from one source. Presumably the court removed this language in view of its potential conflict with the limitations of liability given to a service provider under Section 512(g)(1).

³⁶⁹⁴ Id. at 1059.

³⁶⁹⁵ 2015 U.S. Dist. LEXIS 49999 (C.D. Cal. Jan. 16, 2015).

³⁶⁹⁶ The court's rulings with respect to direct liability are set forth in Section II.A.4(cc) above.

offenders.³⁶⁹⁷ Rosen argued that eBay had not adequately informed its users of its termination policy because users were not told the details of that policy. The court ruled that Section 512(i) does not require that a service provider reveal its decision-making criteria to its users, rather only that it put users on notice that they face exclusion from the service if they repeatedly violate copyright laws.³⁶⁹⁸ Further, “the implementation of a policy need not be perfect to render it sufficient to qualify a service provider for protection under §512(c).”³⁶⁹⁹

The court also rejected Rosen’s argument that eBay had not provided full documentation of all terminations and therefore had not proved that there were not other repeat infringers whom eBay failed to terminate. In the absence of admissible evidence that eBay’s policy was not in fact reasonably implemented, Rosen had offered only conjecture for the possibility that eBay may have failed to “suspend” some repeat infringers, which was insufficient to establish a genuine dispute of material fact.³⁷⁰⁰ Rosen also argued that eBay had not established that it adequately published its repeat infringer policy to users. The court rejected this argument. eBay submitted testimony that it had on its web site a number of policies that informed users of its intellectual property policies, including that repeat offenses might result in “suspensions.” The court ruled that the law does not require eBay to provide its users with a detailed version of its policy, including all of the criteria it uses to determine whether an account will be “suspended.” Rather, all a service provider need do to qualify under Section 512(i) is put users on notice that they face exclusion from the service if they repeatedly violate copyright laws. There was no disputed issue of material fact that eBay had done so.³⁷⁰¹

The court then turned to eBay’s compliance with the requirements of Section 512(c) itself. Rosen challenged whether eBay had provided accurate information as to its designated DMCA officer, in part because it had not identified the name of a specific individual. The court noted that eBay had provided facsimile, telephone, email and mail contact information for its agent, although the agent was not mentioned specifically by name. The court determined that the information provided was sufficient for eBay to have “substantially” provided the necessary information to the public.³⁷⁰² Rosen also argued that eBay failed to expeditiously remove infringing items because, despite taking down the listing, it still kept copies of the copyrighted images on its servers. eBay argued that it had legitimate reasons for keeping copies of the images for some period after taking down the listings – including to allow reposting in response to a counter-DMCA notice – and that once a listing was taken down, eBay had disabled all meaningful public access to the images as required by the safe harbor. The court agreed, noting

³⁶⁹⁷ *Id.* at *2, *19-20. It is curious that eBay’s declarations stated that it had “suspended” repeat offenders, when Section 512(i) requires termination of repeat offenders in appropriate circumstances.

³⁶⁹⁸ *Id.* at *20.

³⁶⁹⁹ *Id.*

³⁷⁰⁰ *Id.* at *20-21. The court’s reference to failure to “suspend” repeat infringers, rather than “terminate” repeat infringers, is again curious.

³⁷⁰¹ *Id.* at * 23-24.

³⁷⁰² *Id.* at *25-26.

that even if Rosen was able to access the image directly, to do so he had to use the unique URL of the image taken from the listing while it was still live. Because it would not be possible for others to access the stored version of the image after the delisting short of copying the URL while the listing was live, eBay had adequately disabled access to the images when it took down the listings.³⁷⁰³

Finally, Rosen argued that eBay was not entitled to the safe harbor because it had the right and ability to control the infringing conduct and received a direct financial benefit from it. The court noted that, under the Ninth Circuit's decision in UMG Recordings, Inc. v. Shelter Capital Partners LLC,³⁷⁰⁴ in order to establish that eBay had the right and ability to control the infringing conduct, Rosen must establish that eBay exerted substantial influence on the activities of users, such as high levels of control over activities of users or purposeful conduct – i.e., something more than required by common law vicarious liability. eBay's mere ability to block or remove access to its web site was not sufficient to establish the requisite right and ability to control. Rosen argued that eBay's requirement that users post a picture, and its requirements as to the picture's size and quality, meant that eBay exerted control over what was posted on its web site. The court ruled that these requirements did not meet the standard for establishing high levels of control over activities of users. eBay did not direct users what to list, did not come into contact with the items being posted, and beyond the basic content requirements, including the photograph requirement, had no control over what its users listed until the listing was complete. Because of eBay's lack of control, the court determined that it need not address whether eBay received a direct financial benefit from the infringing activity. Accordingly, the court granted eBay summary judgment under the Section 512(c) safe harbor.³⁷⁰⁵

ee. Capitol Records v. Escape Media

The facts of this case are set forth in Section III.C.1(c) above. A magistrate judge recommended a finding that the defendant Escape Media was not entitled to the DMCA safe harbor as a matter of law.³⁷⁰⁶ Escape objected to this recommendation, so the district court reviewed it *de novo* and reached the same conclusion.³⁷⁰⁷

The parties agreed that the relevant repeat infringer policy for purposes of the safe harbor was Escape's "one strike policy," not the policy set forth in its Terms of Service. Under its one strike policy, Escape purported to disable account holders' upload privileges in response to DMCA notifications, but did not delete all data or audio files associated with their account or bar them from signing in to simply and passively use the Grooveshark web site. Escape objected to

³⁷⁰³ Id. at *27-30.

³⁷⁰⁴ 718 F.3d 1006, 1030 (9th Cir. 2013).

³⁷⁰⁵ eBay, 2015 U.S. Dist. LEXIS 49999 at *31-35, *53.

³⁷⁰⁶ Capitol Records, LLC v. Escape Media Group, Inc., 2014 U.S. Dist. LEXIS 183098 at *81-124 (S.D.N.Y. May 28, 2014).

³⁷⁰⁷ Capitol Records, LLC v. Escape Media Group, Inc., 2015 U.S. Dist. LEXIS 38007 at *2 (S.D.N.Y. Mar. 25, 2015).

two conclusions reached by the magistrate – that this policy of only barring uploading privileges while retaining accounts did not constitute a repeat infringer policy within the requirements of Section 512(i), and even assuming it did, Escape did not reasonably implement the policy because it did not terminate user’s uploading privileges in appropriate circumstances. In addressing Escape’s objections, the district court found three features of Escape’s policy and implementation to be of particular relevance: Escape’s failure to keep adequate records of infringement; its practice of actively preventing copyright owners from collecting information necessary to issue DMCA takedown notifications; and its failure to terminate repeat infringers.³⁷⁰⁸

Turning first to the issue of Escape’s recordkeeping, the district court noted that prior to the magistrate’s report, Escape had consistently argued that it did not need to track repeat infringement because repeat infringement could not occur under its one strike policy. Before the district court, however, Escape retreated from that position, insisting that it did maintain records in a database of every DMCA takedown processed, including the associated users. The district court noted, however, that Escape provided no admissible evidence showing that it actually tried to identify repeat infringers who were using Grooveshark. Escape’s database of deleted user files did not distinguish between files deleted due to DMCA takedown notices and files deleted due to other reasons, so the database was not an independent record of infringement. Because Escape purposefully failed to keep adequate records of repeat infringement, it did not “implement” a repeat infringer policy as required by Section 512(i).³⁷⁰⁹

Moreover, the court found that Escape employed a practice that prevented copyright owners from being able to identify repeat infringements in the first place. Grooveshark’s site organized multiple files containing the same song together, but only the “Primary File” could be streamed by Grooveshark users. When Escape received a DMCA takedown notice for files that infringed a copyrighted work, only the Primary File linked to a song was removed, and, if there were Non-Primary Files associated with that same song, the song remained available to Grooveshark users because a new Primary File would be selected automatically from the Non-Primary Files the next time the song was selected for streaming. This process of selecting a Non-Primary File as a replacement Primary File for streaming would continue until there were no remaining Non-Primary Files for that particular song. Because it was not possible for content owners to obtain URLs for Non-Primary Files, and because the only URL visible to users and content owners was the URL for the Primary File for a song, content owners had to submit successive takedown notices even for Non-Primary Files slotted behind Primary Files that had already received takedown notices. Such process therefore actively prevented copyright owners from collecting information needed to issue DMCA notices in a manner that would have any meaningful consequence, which the district court ruled was an independent basis for concluding that Escape did not “implement” a repeat infringer policy as Section 512(i) requires.³⁷¹⁰

³⁷⁰⁸ Id. at *13-14.

³⁷⁰⁹ Id. at *15-18.

³⁷¹⁰ Id. at *18-22.

The court next turned to what it considered to be an even more fundamental issue – that as implemented, Escape’s policy did not actually provide for the termination of repeat infringers. Under Escape’s one strike policy, the most severe consequence for a repeat infringer was a loss of his or her uploading privileges – Escape had not and would not terminate a repeat infringer’s account regardless of the level of repeat infringement. The court noted that the common definition of the word “termination” suggests that Congress intended service providers to have a policy in place that would end or discontinue the accounts of repeat infringers, not something short of that such as limiting repeat infringers’ user privileges. Escape’s one strike policy prevented only the uploading of *content*, but did not provide for the termination of *account holders*, as Section 512(i) requires. In sum, in view of Escape’s improper recordkeeping, its “Primary File” practices, and its failure to actually terminate repeat infringers each provided independent ground for finding that Escape did not “implement” a repeat infringer policy.³⁷¹¹

Finally, the district court ruled that, even if Escape’s one strike policy could satisfy Section 512(i)’s implementation requirement, its implementation of that policy was not reasonable. The relevant question was whether Escape actually terminated the uploading privileges of repeat infringers under appropriate circumstances. The court noted the magistrate’s finding of multiple examples of Escape’s failure to bar the uploading privileges of repeat infringers. The most troubling example was Escape’s “DMCA Lite” procedure under which, if Escape received a DMCA takedown notice, but concluded that it was defective (e.g. because it was not signed under oath or did not adequately identify the location of the alleged infringement on Grooveshark), it would not disable the user’s uploading capability. The court noted that, to be effective under the DMCA, a notice need only include “substantially” six components delineated in Section 512(c)(3)(A). Since Feb. 13, 2013, Escape had removed only 6,861 files, but 94.2% of those had been removed under its DMCA Lite procedure. The fact that Escape deemed 94.2% of DMCA notices defective, but was still able to identify and remove the files, belied its contention that the notices did not “substantially” comply with Section 512(c)(3)(A). Similarly, Escape offered no admissible evidence demonstrating how the vast majority of DMCA takedown notices were effective enough for it to identify the user-submitted file, but so defective that they did not warrant terminating the user’s uploading privileges.³⁷¹²

The court went on to observe that perhaps the strongest indicator of Escape’s failure to terminate the uploading privileges of repeat infringers in appropriate circumstances was the undisputed facts showing that hundreds or thousands of users were not stripped of their uploading privileges after receiving notices of infringement. Notably, 1,609 users received DMCA notices for an upload that occurred after the user had already received a prior DMCA notice. Those 1,609 users submitted 2,339,671 files that were still available in Grooveshark’s active library. And at least 3,323 users for whom there was documentation of infringement in Escape’s database still had their uploading privileges enabled. The court found the failure of Escape’s purported one strike policy to be all the more alarming in view of the fact that 21,044 users who had received multiple DMCA notices accounted for 7,098,634 uploads, or 35% of all

³⁷¹¹ *Id.* at *22-29.

³⁷¹² *Id.* at *29-31.

uploads to Grooveshark's active music library. Escape therefore had no effective mechanism for tracking subsequent infringing uploads by users who purportedly had their uploading privileges suspended.³⁷¹³

The court concluded that, because Escape had not shown its satisfaction of the Section 512(i) eligibility conditions, no reasonable jury could conclude that Escape was entitled to the Section 512(c) safe harbor. And for that reason, the court found that it need not reach the plaintiff's alternative arguments that Escape did not satisfy the remaining requirements of Section 512(c), nor whether the DMCA safe harbor extends to sound recordings fixed prior to 1972.³⁷¹⁴

ff. BWP Media v. Clarity Digital

The District Court Decision

In this case, the defendant operated the Examiner.com website where visitors could access articles on a variety of topics including arts, entertainment, news, sports, and technology. The plaintiffs were the owners of photographs that they licensed for use by online and print publications. The plaintiffs accused the defendant of copying, posting or displaying 75 of their photographs without authorization. The defendant moved for summary judgment under the Section 512(c) safe harbor.³⁷¹⁵

The plaintiffs claimed that the defendant was not entitled to the safe harbor because the photos were not posted by "users" of the Examiner.com website, but rather by the defendant itself, based on the following facts. The defendant recruited individuals to contribute articles to its site called "Examiners." To become an Examiner, an individual was required to file an application with a writing sample and undergo a background check. Examiners signed an independent contractor agreement with the defendant requiring them to use their best efforts to create works on a topic for a specific Examiner.com edition, maintain their topic page, publish works to the topic page using the Examiner.com publishing application, create an online community relating to their topic page, drive legitimate traffic to the topic page, and regularly create and post new works to their topic page and update it as often as reasonably needed. The agreement also required Examiners to comply with the Examiner.com editorial requirements. Examiners were eligible to be compensated for their posts pursuant to a written payment policy. Once an article was posted on a topic page, the defendant exclusively determined whether it would be featured elsewhere on the site. There was evidence that Examiner.com staff communicated with Examiners regarding the content of their posts.³⁷¹⁶

³⁷¹³ Id. at *31-33.

³⁷¹⁴ Id. at *33-34.

³⁷¹⁵ BWP Media USA Inc. v. Clarity Digital Group, LLC, 2015 U.S. Dist. LEXIS 42211 at *2 (D. Colo. Mar. 31, 2015), aff'd, 820 F.3d 1175 (10th Cir. 2016).

³⁷¹⁶ Id. at *2-9.

The plaintiffs asserted that the defendant should not be entitled to the safe harbor because the Examiners were not “users” under Section 512(c). The plaintiffs argued the term “user” should exclude a service provider’s owners, employees and agents, as determined by reference to traditional principles of agency law. The court rejected this narrow interpretation of the word “user,” noting that Section 512(c) does not define “user,” and its plain and ordinary dictionary meaning is simply “one that uses.” Accordingly, “user” should mean simply a person or entity who avails itself of the service provider’s system or network to store material. The court noted that both Sections 512(a)(1) and 512(b)(1)(A) utilize the phrase “a person other than the service provider,” so Congress knew how to make the distinction between service providers and third parties through different words other than “user.”³⁷¹⁷

Moreover, the court held that it was not necessary to interpret the term “user” narrowly in order to distinguish between the storage at the direction of the service provider and storage at the direction of third parties. The court found that the service provider behavior the plaintiffs were concerned about is already addressed in subparagraphs (A) through (C) of Section 512(c)(1), where the term “storage” limits a service provider from invoking safe harbor protection for its own conduct because, although “storage” encompasses automated processes for making files accessible, under the Ninth Circuit’s UMG Recordings v. Shelter Capital Partners case, service providers lose protection for activities they undertake that lack a causal connection to user-initiated storage of infringing material. Similarly, under UMG, Section 512(c)(1)(B) excludes the safe harbor for infringing activity that confers a financial benefit upon the service provider if the service provider exerts substantial influence on the activities of users, such as high levels of control over their activities or purposeful conduct. Thus, the court concluded that to define the term “user” narrowly or to read agency principles into the term would, in many instances, be unnecessary and redundant given the effect of Section 512(c)’s other provisions.³⁷¹⁸

Accordingly, the court found that the Examiners were “users” within the meaning of Section 512(c). However, the court noted that the safe harbor protection does not extend to all user-uploaded content, but only to content uploaded “at the direction of a user.” The key question in the present case was then whether the plaintiffs’ photographs were stored on the defendant’s system at the direction of the Examiners or at the direction of the defendant. The court held the photographs were stored at the direction of the Examiners. There was no indication that the defendant directed the Examiners to upload the plaintiffs’ photographs or any other infringing content. The record contained no evidence of any communications between the defendant and the Examiners at issue regarding the plaintiffs’ photographs or the posts in which the plaintiffs’ photographs appeared. The defendant asserted that it did not pre-screen, edit, or approve any of the content at issue before it was posted to the site. Although a dispute of fact may have existed as to whether the defendant had content managers or a review team, there was no evidence suggesting that a content manager, review team, or any Examiner.com staff had any actual control or influence over the content of the articles containing the plaintiffs’

³⁷¹⁷ Id. at *16-19.

³⁷¹⁸ Id. at *19-21.

photographs so as to render the use of the plaintiffs' photographs at the direction of the defendant. Indeed, the Examiner agreement required Examiners to have permission of the owner/copyright holder of any content before including it on a web page and the editorial requirements contained a prohibition on unlicensed content.³⁷¹⁹

The plaintiffs next argued that the defendant did not qualify for the safe harbor because it was willfully blind to infringements occurring on Examiner.com. The court noted that under UMG the willful blindness doctrine may be applied in the context of Section 512(c)(1)(A), but only to the extent the evidence establishes that a service provider willfully buried its head in the sand to avoid obtaining knowledge of the specific infringing activity. The plaintiffs pointed to a series of emails from the defendant to various Examiners requesting photos and videos regarding the Oscars, new TV lineups and premiers, new movies, celebrity scandals, celebrity bodies, celebrity styles, celebrity news and Emmy Awards fashions. The court found that, at best, the emails suggested that the defendant might have had a general awareness that Examiners could post infringing content in response to such requests, but general awareness is insufficient to create a genuine dispute as to whether the defendant had knowledge of or was willfully blind to the specific infringement alleged in the case. Accordingly, there was no evidence specific to any of the claimed infringements upon which a reasonable juror could conclude that the defendant possessed the requisite actual or red flag knowledge to deny the safe harbor.³⁷²⁰

Finally, the court examined the financial benefit prong of the Section 512(c) safe harbor, noting that where, as here, a service provider derives its revenue from advertising, the inquiry focuses on whether the connection between the infringing activity and the service provider's income stream derived from advertising is sufficiently direct. The court concluded that in this case it was not. There was no evidence that the defendant marketed to advertisers by pointing to infringing content, that users considered Examiner.com a reliable source of infringing content, that any users visited Examiner.com because it hosted infringing content, or that the defendant actively promoted infringing content as a way of attracting more page views. As a result, there were no facts supporting an inference that the defendant's revenue stream was in any way predicated on or derived from the availability of infringing material on Examiner.com. Accordingly, the court granted summary judgment that the defendant was entitled to Section 512(c) safe harbor protection.³⁷²¹

The Tenth Circuit's Decision

On appeal, the Tenth Circuit affirmed.³⁷²² The court ruled that the word "user" in the DMCA is straightforward and unambiguous, simply meaning "one who uses." The Tenth Circuit

³⁷¹⁹ Id. at *24-26.

³⁷²⁰ Id. at *27-29.

³⁷²¹ Id. at *30-33.

³⁷²² BWP Media USA, Inc. v. Clarity Digital Group, LLC, 820 F.3d 1175 (10th Cir. 2016).

agreed with the district court that, in the DMCA context, the term “user” describes a person or entity who avails itself of the service provider’s system or network to store material. The Tenth Circuit rejected the plaintiffs’ argument that the ordinary meaning of the term “user” would protect every OSP from liability for copyright infringement. The court noted that an OSP will qualify for safe harbor protection only when it can show, *inter alia*, that it had no actual knowledge of the infringement, that there were no surrounding facts or circumstances making the infringement apparent, or that upon learning of the infringement, the OSP acted expeditiously to remove or disable access to the infringing material.³⁷²³

The plaintiffs also argued that Examiners were agents of the defendant but the court found no evidence supported that, pointing to the fact that the Examiners were expressly designated as independent contractors in the contract between them and the defendant. There was also no evidence to support the plaintiffs’ argument that Examiners had apparent authority and should therefore be treated as employees of the defendant. And in any event, the court concluded, simply because a person is an employee does not automatically disqualify him as a “user” under Section 512.³⁷²⁴

The court elaborated that the relevant question isn’t who the “user” is, but rather, who directed the storage of the infringing content. Key to that determination is the issue of control. There is no protection under Section 512 when the infringing material is on the system or network as a result of the service provider’s own acts or decisions. If the service provider actively encourages infringement by urging its users to both upload and download particular copyrighted works, it will not be entitled to the safe harbor. But if the infringing content has merely gone through a screening or automated process, the service provider will generally benefit from the safe harbor. The court rejected the plaintiffs’ argument that the defendant directed Examiners to post the infringing content by issuing instructions on the general topics Examiners were to write about, actively soliciting new articles, and suggesting that Examiners include slide shows or pictures to accompany articles. The court noted that not only did the defendant make clear copyright infringement was prohibited, it also provided Examiners with licensed photographs to accompany their articles.³⁷²⁵

The plaintiffs further argued that because photographs of celebrities are typically protected by copyright and the defendant knew celebrity images were being posted on Examiner.com, it was willfully blind to the copyright infringement. The court rejected this argument, noting that there was nothing in the record showing the defendant ignored signs or circumstances suggesting copyright infringement was occurring on Examiner.com. Although the defendant encouraged Examiners to incorporate photographs into articles, it provided Examiners a legal means by which to do so in the form of a photo bank of licensed photographs.

³⁷²³ Id. at 1179-80.

³⁷²⁴ Id. at 1180-81.

³⁷²⁵ Id. at 1181.

Accordingly, the Tenth Circuit affirmed the district court's ruling that the defendant was entitled to the Section 512(c) safe harbor.³⁷²⁶

gg. Milo & Gabby v. Amazon.com

In this case, the plaintiffs were owners of copyrights in a line of animal shaped pillowcases that functioned as a combination between a pillow and a stuffed animal. The plaintiffs alleged that Amazon offered and sold knockoff copies of its pillowcases offered by third party sellers on Amazon.com and sued it for infringement of its exclusive rights of public display and distribution. Upon receipt of the complaint, Amazon investigated and removed within days the allegedly infringing pillowcase offerings from its site. During the course of the lawsuit, additional third party sellers offered allegedly infringing pillowcases on the site, which Amazon also promptly removed. Amazon moved for summary judgment under the Section 512(c) safe harbor.³⁷²⁷

The court first turned to the plaintiffs' claim for direct copyright infringement against Amazon. The court found that the allegedly infringing images of the plaintiffs' copyrighted pillowcases stored on the website were provided by a third-party vendor and were handled in an entirely automated manner to generate product detail pages or ads for the allegedly infringing pillowcases. Amazon's acceptance and storage of the allegedly infringing images depicting the knockoff pillowcases was insufficient to hold it directly liable. Direct copyright infringement requires that the defendant have actively engaged in one of the protected activities under the Copyright Act. Here, the unrebutted evidence in the record demonstrated that the content of the detail pages and ads was supplied by third parties via an automated file upload system, and did not originate from Amazon. Thus, Amazon had not actively participated in the alleged copying of the digital images at issue and was thus not directly liable.³⁷²⁸

The court then turned to Amazon's assertion of the Section 512(c) safe harbor. The plaintiffs did not dispute that Amazon had adopted and informed its users of a policy that provided for the termination of users who were repeat infringers, and that it had reasonably implemented its policy because it provided mechanisms for the filing of claims of infringement, a process for removal of infringing products, and processes for the permanent suspension of repeat offenders. With respect to the knowledge requirement, Amazon had presented evidence that it did not have actual notice of infringement before the lawsuit was filed, but the plaintiffs argued that Amazon did have notice. The court ruled, however, that regardless of whether the plaintiffs could establish actual notice, Amazon had acted expeditiously to remove the allegedly infringing material in response to the lawsuit, and there was no evidence in the record to the contrary.³⁷²⁹

³⁷²⁶ Id. at 1182.

³⁷²⁷ Milo & Gabby, LLC v. Amazon.com, Inc., 2015 U.S. Dist. LEXIS 92890 at *2, *5-7 (W.D. Wash. July 16, 2015).

³⁷²⁸ Id. at *11, *14-15.

³⁷²⁹ Id. at *19-22.

The court then turned to the control and financial benefit prongs of the safe harbor. Under Ninth Circuit law pertaining to the control prong, the court noted that a service provider must exert substantial influence on the activities of users. The court further noted that under Ninth Circuit law a service provider does not have the practical ability to stop or limit infringing conduct simply because (1) the infringing content resides on the service provider's system; (2) the service provider had the ability to remove such material; (3) the service provider could have implemented, and did not implement, filtering systems; and (4) the service provider could have searched for potentially infringing content. Rather the law requires something more, and in this case, the court agreed with Amazon that the plaintiffs had failed to identify the "something more" such that Amazon had the *practical ability* to control infringement. It was undisputed that Amazon lacked the ability to analyze every image it received from third party sellers, compare the submitted image to all other copyrighted images that exist in the world, and determine whether each additional image infringed someone's copyright interest. As a result, Amazon lacked the ability to control the infringing activity. Because Amazon lacked control, it was not necessary for the court to determine whether Amazon received a direct financial benefit from the allegedly infringing conduct. Accordingly, the court ruled that Amazon was entitled to the safe harbor and dismissed the plaintiffs' copyright claim in its entirety.³⁷³⁰

hh. Hempton v. Pond5

In Hempton v. Pond5, Inc.,³⁷³¹ the plaintiff, Gordon Hempton, was the owner of copyrights in thousands of recordings of natural sounds. The defendant operated the Pond5 web site that hosted a wide variety of digital media that customers could purchase licenses for. Hempton discovered hundreds of his natural sound recording files being offered for sale on the Pond5 web site by a Pond5 customer whose ID was ckennedy342. Hempton's counsel sent a letter to Pond5 demanding that it take down all files offered by ckennedy342. The next day, Pond5 suspended ckennedy342's account and removed all of his content from the Pond5 web site. Hempton then initiated a copyright infringement suit against Pond5 and ckennedy342. Pond5 moved for summary judgment under the Section 512(c) safe harbor.³⁷³²

Hempton argued that Pond5 was not eligible for the safe harbor because it had not adopted nor reasonably implemented a policy for termination of repeat infringers. The court rejected this argument. It found that Pond5 had adopted and reasonably informed its users of a policy providing for the termination of service access for repeat copyright infringers in appropriate circumstances. Pond5's Terms of Service, which each user was required to accept before uploading content to the web site, required users not to send or upload any content that infringed anyone else's copyright or other legal right, and informed users that Pond5 could at its sole discretion terminate or limit anyone's access to or use of its web site for failure to comply

³⁷³⁰ Id. at *22-25. The court also rejected a claim that Amazon had violated the DMCA by intentionally removing or altering copyright management information from their copyrighted images because plaintiffs' had failed to point to any evidence in the record rebutting Amazon's assertions that it had not done so. Id. at *24-25.

³⁷³¹ 2016 U.S. Dist. LEXIS 147830 (W.D. Wa. Oct. 25, 2016).

³⁷³² Id. at *1-9.

with any provision of the Terms of Use. The fact that Pond5 allowed for such termination for any violation of its terms, rather specifically limiting termination to repeat infringers, was immaterial. Pond5 had gone beyond the threshold requirement of the DMCA by communicating a policy to its users that allowed for termination for any infringement. The court concluded that Pond5 had reasonably implemented its policy in view of evidence it put forth that from 2012 to 2016, it received 20 DMCA takedown notices and it removed the challenged content in every instance.³⁷³³

Hempton further argued that Pond5 was not eligible for the safe harbor because it had red flag knowledge of infringement and failed to act. The court rejected this argument, relying on Ninth Circuit authority essentially equating red flag knowledge to willful blindness: “Thus, a service provider may have ‘red flag’ warning of specific infringement under § 512(c)(1)(A)(ii), but only to the extent the evidence establishes that a service provider ‘willfully bur[ied] its head in the sand to avoid obtaining ... knowledge of specific infringing activity.’”³⁷³⁴ Hempton alleged willful blindness because Pond5 was allegedly aware that the individual behind the user name ckennedy342 – Hassan Kahn – had in 2014 uploaded infringing nature audio videos to Pond5’s web site under the user name “WildAudioProduction.” Pond5 became suspicious of WildAudioProduction in May 2014 and shortly thereafter tagged both Kahn and WildAudioProduction as infringers and terminated both accounts. The ckennedy342 account was thereafter created in August 2014. The IP address associated with ckennedy342 was the same IP address in Pakistan that was used by Kahn and WildAudioProduction. In addition, the ckennedy342 account was linked to a Paypal account registered to the name Hassan Khan. Hempton argued that these facts constituted “red flag” awareness of ckennedy342’s infringement.³⁷³⁵

The court rejected this argument, noting that Hempton misrepresented the extent of Pond5’s knowledge regarding ckennedy342 in 2014. Although Pond5 admitted it discovered that Hassan Kahn used the WildAudioProduction user name in May 2014 and that ckennedy342 created an account in August 2014, that was the extent of Pond5’s knowledge about ckennedy342 in 2014. It did not know that the IP address login for ckennedy342 was the same as the IP address login for Hassan Kahn and WildAudioProduction because Pond5 did not conduct IP address checks in 2014. Nor did Pond5 know that ckennedy342 was from Pakistan and could not have discovered that information without an investigation, something Pond5 was not required to do under the DMCA. And Pond5 presented testimony that it did not perform a comparison of names used in PayPal or other payment accounts to other contributors to the web site.³⁷³⁶

³⁷³³ Id. at *12-19.

³⁷³⁴ Id. at *23-24 (quoting UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1023 (9th Cir. 2013)).

³⁷³⁵ Hempton, 2016 U.S. Dist. LEXIS 147830 at *24-25.

³⁷³⁶ Id. at *25-28.

Finally, Hempton asserted that Pond5 was not entitled to the safe harbor because Pond5 received a financial benefit from the infringing activity in ckennedy342's account in the amount of between \$192.95 and \$2,000. The court rejected this argument, finding no facts to support an inference that Pond5's revenue stream was in any way predicated on or derived from the availability of infringing material on its site. Specifically, there was no evidence that any customer had ever visited the site because it hosted infringing content, nor was there any evidence that Pond5 had ever promoted infringing content. There was also no evidence that Pond5 conducted marketing by pointing to infringing conduct or that Pond5 provided a significant source of infringing content in the marketplace. The court therefore concluded there was a complete absence of any causal connection between any alleged financial benefit and any infringing activity. Accordingly, the court granted Pond5's motion for summary judgment under the safe harbor.³⁷³⁷

The court subsequently denied a motion for reconsideration by Hempton on the grounds of two expert reports that Hempton produced cataloguing the many red flags in the ckennedy342 sound files, track names, and metadata. The court cited multiple authority holding that what constitutes a red flag is judged on an objective standard (whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances), and therefore an issue of material fact cannot be created under that standard through the submission of expert testimony.³⁷³⁸ "If expert testimony is required to determine what constitutes a red flag, by definition, it would not be a red flag to the ordinary person."³⁷³⁹

ii. Greg Young Publishing v. Zazzle

In Greg Young Publishing, Inc. v. Zazzle, Inc.,³⁷⁴⁰ the defendant Zazzle ran a web site that allowed users to upload images of artwork, slogans, and designs. Users could choose various consumer products they wanted the image to appear on, such as coffee mugs, posters and t-shirts, and offer those products for sale to the public. When an order was placed, Zazzle produced and delivered the product, paying a royalty to the user who uploaded the image appearing on the product. The plaintiff alleged that Zazzle publicly displayed without authorization 41 paintings and created consumer products bearing those images, for which the plaintiff asserted copyright infringement.³⁷⁴¹

The plaintiff moved for summary judgment that Zazzle was not entitled to the Section 512(c) safe harbor because Zazzle was not a service provider, Zazzle knew its services were being used to infringe the plaintiff's copyrights, and Zazzle received a financial benefit from the infringing activity and had the right and ability to control it. The court rejected the plaintiff's first

³⁷³⁷ Id. at *29-32.

³⁷³⁸ Hempton v. Pond5, Inc., 2017 U.S. Dist. LEXIS 5724 at *5-6 (W.D. Wa. Jan. 13, 2017).

³⁷³⁹ Id. at *7.

³⁷⁴⁰ 2017 U.S. Dist. LEXIS 100268 (C.D. Cal. 2017).

³⁷⁴¹ Id. at *2.

argument, finding that Zazzle offered online services in the form of operation of a web site that allowed users to upload images to print on consumer products and the sale of products bearing images from Disney, Warner Bros., Marvel and other popular brands, which made it a service provider for purposes of Section 512(c).³⁷⁴²

With respect to the plaintiff's second argument, the court acknowledged that a service provider is not eligible for the safe harbor if it is aware of facts or circumstances from which infringing activity is apparent and takes no action. However, the court observed that this constructive knowledge clause has been construed so narrowly in the Ninth Circuit that it is questionable whether it retains any independent meaning.³⁷⁴³ According to the court, under Ninth Circuit precedent, a service provider will not be found to have knowledge of infringement "unless (1) the copyright holder submits a complaint that complies with the DMCA's procedural requirements (a deficient notice cannot be used to establish knowledge); or (2) a third-party submits a sufficiently specific complaint about potential infringement."³⁷⁴⁴ The plaintiff argued that Zazzle knew its users were uploading the plaintiff's images because it had complained about the infringement and provided Zazzle with a catalog of its images to be used to check for future incidents of infringements. The court noted that, even if true, such fact did not render Zazzle ineligible for the safe harbor because the plaintiff offered no evidence that Zazzle had specific knowledge of particular infringing activity and nonetheless failed to take corrective action with respect to that activity.³⁷⁴⁵

With respect to the plaintiff's third argument, the court noted that under UMG Recordings, Inc. v. Shelter Capital Partners LLC,³⁷⁴⁶ a service provider will not be found to have the right and ability to control the activities of its users unless it exerts "substantial influence" over those activities, and such influence will be found where the service provider plays an active role in selecting, monitoring, or marketing user content. Here, the court concluded that Zazzle had the right and ability to control the types of products it produced because, as the plaintiff argued, it was actively involved in selecting the products that were sold, pricing and selling the products, manufacturing the products, and packaging and delivering the products. The court rejected Zazzle's argument that it lacked the ability to control the sale of infringing products because, in practice, the production process was effectively automatic after a product was ordered and approved by Zazzle's content management team. The court ruled it did not matter if Zazzle lacked the ability to control its production process after the content management team approved the product, because presumably that team had the authority to reject products that were infringing. But more to the point, even if the entire process were automatic, that would

³⁷⁴² Id. at *15-16. The court found the reasoning of Agence France Presse v. Morel, 934 F. Supp. 2d 547 (S.D.N.Y. 2013), to be unpersuasive and an "outlier" case in its treatment of the definition of "service provider" as a meaningful restriction on the applicability of Section 512(c). Zazzle, 2017 U.S. Dist. LEXIS at *16.

³⁷⁴³ Id. at *18.

³⁷⁴⁴ Id. at *19.

³⁷⁴⁵ Id.

³⁷⁴⁶ 718 F.3d 1006, 1030 (9th Cir. 2013).

suggest at most that Zazzle had chosen not to exercise its right and ability to reject infringing products, not that it lacked the right or ability to do so. The plaintiff was therefore entitled to summary judgment that Zazzle was not protected under Section 512(c) to the extent it manufactured and sold physical products bearing infringing images. However, Zazzle was not precluded from invoking Section 512(c) with respect to images that were displayed on its web site but never printed onto physical products, because it was not clear that Zazzle received a financial benefit from merely displaying images on its web site, or that Zazzle had the right or ability to control the types of images its users uploaded.³⁷⁴⁷

jj. Long v. Dorset

The plaintiff set up a web page on Facebook devoted to yoga. One of the defendants, a hacker, accessed the web page and changed the administrative passwords, establishing himself or herself as the administrator and locking out the plaintiff. The hacker posted copyrighted images owned by the plaintiff on the web page and configured those posts so that when a user clicked on the copyrighted material, the user would be redirected to a web site that closely resembled the plaintiff's blog. The fake blog contained pornographic advertisements and attempted to install malicious malware on the user's device. The plaintiff sent a series of emails to Facebook, stating that his web page had been hacked, that the plaintiff was the rightful owner of the page, and that the hacker was posting infringing materials. Some of the plaintiff's emails stated that the email constituted official notification under Section 512(c) of the DMCA, and some of them attached screenshots of copyrighted material the hacker had posted. Facebook replied with an email that sought clarification of whether the plaintiff was making an intellectual property claim or writing about a page administration issue. Over the next several days, the plaintiff and Facebook continued to exchange emails about those issues. Five days after the hacker hacked the plaintiff's Facebook page, Facebook restored the plaintiff's administrator status to the page. Although this restoration resolved the alleged infringement occurring on Facebook's platform, the plaintiff sued Facebook for copyright infringement and other causes of action.³⁷⁴⁸

Facebook brought a motion to dismiss the copyright claims based on the Section 512 safe harbors. In opposition, the plaintiff argued only that the safe harbors did not protect Facebook because it failed to act expeditiously in response to the plaintiff's DMCA notices. The court noted that it was an issue of first impression whether the question of expeditiousness can be decided on a motion to dismiss. Noting that numerous cases had granted summary judgment based on the defendant's compliance with the expeditiousness requirement, the court saw no reason why the issue could not also be resolved on a motion to dismiss. In addition, the court found that the purpose of the DMCA would be undermined if the issue of expeditiousness could not be resolved, when appropriate, as a matter of law, since Congress enacted the DMCA to

³⁷⁴⁷ Zazzle, 2017 U.S. Dist. LEXIS at *20-23.

³⁷⁴⁸ Long v. Dorset, 369 F. Supp. 3d 939, 942-43 (N.D. Cal. 2019).

provide greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.³⁷⁴⁹

The court noted that, although the issue of expeditiousness will not always be ripe for decision at the motion to dismiss stage, on the facts of the case here, it was. The court found that Facebook's five business day response satisfied the expeditiousness requirement. The plaintiff sought the removal of over a hundred allegedly infringing images and also sought the restoration of his administrator status. Facebook promptly responded to the plaintiff's initial email and, over the next several days, continued to exchange emails with the plaintiff to resolve the issues. After five business days, Facebook had resolved the plaintiff's complaint. Based on those allegations, the court ruled that the safe harbors applied to the plaintiff's copyright claims because Facebook satisfied the expeditiousness requirement as a matter of law, and granted Facebook's motion to dismiss the copyright infringement claims.³⁷⁵⁰

In subsequent litigation, a district court dismissed the plaintiff's claims of direct, contributory and vicarious liability against Facebook with prejudice.³⁷⁵¹ The Ninth Circuit affirmed in a brief opinion designated not appropriate for publication. The Ninth Circuit rejected the plaintiff's argument that Facebook's failure to promptly remove the hacker's posts amounted to volitional conduct. The court noted that it had rejected such failure-to-act arguments when, as here, an online service provider took affirmative actions to address the claims by requesting further information from the copyright holder upon being informed of potential infringement. The court rejected the plaintiff's vicarious infringement claim, finding the plaintiff's allegations that he paid Facebook to post advertisements for his business page on users' newsfeeds did not suffice as allegations that Facebook made money from the hacker's infringing posts on that page specifically. And it affirmed the dismissal of the plaintiff's contributory claim, finding that the plaintiff's allegations failed to plausibly establish that Facebook actually knew precisely what infringing material was available on Facebook. The court noted, however, that the plaintiff might be able to plead facts describing other communications to Facebook that clearly identified a set of specific infringing images on Facebook. Accordingly, the court vacated the district court's order dismissing the contributory infringement claim with prejudice, directing that the plaintiff should be given leave to amend.³⁷⁵²

In subsequent proceedings, the plaintiff did amend its contributory claim, but the district court again dismissed the claim with prejudice, finding that the plaintiff had not in fact alleged any other communications not previously alleged in its earlier complaint.³⁷⁵³

³⁷⁴⁹ Id. at 945-46.

³⁷⁵⁰ Id. at 947, 949.

³⁷⁵¹ Long v. Dorset, 2021 U.S. Dist. LEXIS 255851 (N.D. Cal. May 21, 2021).

³⁷⁵² Long v. Dorset, 2021 U.S. App. LEXIS 12095 at *2-5 (9th Cir. Apr. 23, 2021).

³⁷⁵³ Long v. Dorset, 2021 U.S. Dist. LEXIS 177624 at *6-10 (N.D. Cal. Sept. 17, 2021).

kk. Downs v. Oath

Downs was a professional photographer whose photo was used without his permission in connection with an article posted on HuffPost, owned and operated by the defendant Oath Inc. The article was written and uploaded by a third party participant on HuffPost's "contributor" platform. The day after the author posted her article, a HuffPost editor screened the article for offensive or unlawful content and added content tags to the article's metadata and a "related video" link beneath the article. Downs sued for copyright infringement and Oath moved for summary judgment on its Section 512(c) safe harbor defense.³⁷⁵⁴

The court ruled that the editor's cursory screening and modification of the article did not place it outside of the safe harbor. The court distinguished Mavrix v. LiveJournal,³⁷⁵⁵ the only case on which Downs relied, because in that case the defendant chose a small subset of user submissions to post publicly. Here, contributors published their articles directly to HuffPost. Nor did the addition of content tags deprive Oath of immunity, as the safe harbor extends to software functions performed for the purpose of facilitating access to user-stored material, which purpose the tags fulfilled.³⁷⁵⁶

The court rejected Downs' argument that HuffPost had red flag knowledge of infringement because the photo in the article had a New York Daily News credit. Disqualification for red flag knowledge requires that the service provider have actually known facts that would make the specific claimed infringement objectively obvious to a reasonable person, and the copyright owner bears the burden to make that showing. The reasonable person of relevance under the standard is one not endowed with specialized knowledge or expertise concerning the laws of copyright. Here, the court concluded that infringement would not have been so obvious. The editor's viewing of Downs' photo may have been brief, and the editor was viewing the article for multiple purposes, including subject matter classification and screening for offensive content. While it was possible the editor saw the New York Daily News photo credit, that possibility was not enough to create a triable issue as to red flag knowledge. Downs had failed to take discovery or otherwise adduce evidence sufficient to make his required showing that the editor had acquired knowledge of facts and circumstances from which infringing activity was obvious. Nor could the editor be expected to distinguish between infringements and fair or authorized uses. Accordingly, Downs had failed to create a triable issue as to red flag knowledge.³⁷⁵⁷

Finally, Downs argued that HuffPost received a financial benefit directly attributable to the infringement from the commercial ads that were visible on the face of the article and that Oath had the right and ability to control the article because HuffPost engaged in human supervision and review of content posted to the web site. The court rejected these arguments.

³⁷⁵⁴ Downs v. Oath Inc., 385 F. Supp. 3d 298, 300-01 (S.D.N.Y. 2019).

³⁷⁵⁵ This case is discussed in Section III.C.6(b)(1)(iii).cc above.

³⁷⁵⁶ Id. at 304-05.

³⁷⁵⁷ Id. at 305-07.

It was not enough that HuffPost ran commercial ads on its web site – if that were sufficient, then practically every revenue-generating web site would satisfy the financial benefit prong. Instead, Downs was required to put forth evidence of a connection between the allegedly infringing activity and the financial benefit that HuffPost received. Here, Downs made no such showing. There was no evidence that HuffPost encouraged infringement, that it promoted ads by pointing to infringement, or that its users primarily engaged in infringing conduct. Nor was the ability to remove or block access to materials posted on its web site sufficient under applicable Second Circuit authority. The right and ability to control contemplates circumstances in which a service provider exerts substantial influence on the activities of users. Here, the undisputed evidence showed that contributors self-published their articles directly to the web site and that HuffPost engaged in only cursory screening and modification. Such level of involvement was insufficient as a matter of law to establish right and ability to control infringing activity by members of its contributor platform. Accordingly, the court granted Oath’s motion for summary judgment and ordered the case dismissed.³⁷⁵⁸

II. Feingold v. RageOn

The defendant operated a platform that allowed vendors to design merchandise and sell it to consumers through the defendant’s online marketplace. The plaintiff sued the defendant for copyright infringement based on the defendant’s offering for sale through its marketplace three T-shirt varieties bearing the image of one of the plaintiff’s copyrighted photographs and one T-shirt variety bearing the images of a second one of the plaintiff’s copyrighted photographs. The court ruled that the defendant did not qualify for the protections of the Section 512(c) safe harbor for at least two reasons. First, the defendant received a financial benefit directly attributable to the infringing activity, in the form of revenue from the sale of infringing merchandise. The defendant had the right and ability to control that activity – because the defendant was an online retailer, common sense dictated that it had the right and ability to control what it sold, and the defendant offered not evidence to the contrary. Second, the defendant did not expeditiously remove the infringing merchandise. The defendant admitted that it took 18-23 days to remove the T-shirts infringing the plaintiff’s first photograph, and at least 18 days to remove the T-shirts infringing the plaintiff’s second photograph – despite initial assurance in both cases to the plaintiff’s counsel that it would act within 24 hours.³⁷⁵⁹

mm. Williams-Sonoma v. Amazon.com

For an analysis of this case and Amazon’s assertion of a Section 512(c) defense against allegations of direct infringement based on unauthorized photos posted on product detail pages for items for sale by sellers on its online marketplace, see Section II.A.4(ee) above.

nn. Atari v. Redbubble

³⁷⁵⁸ Id. at 307-08.

³⁷⁵⁹ Feingold v. RageOn, Inc., 472 F. Supp. 3d 94, 97, 102 (S.D.N.Y. 2020).

(For a discussion of Section 512(c) safe harbor issues in this case, see Section III.C.1(j) above.)

(iv) Referral or Linking to Infringing Material (Information Location Tools) – Section 512(d)

Section 512(d) provides that a Service Provider is not liable for monetary relief, and is subject only to limited injunctive relief, for referring or linking users to an online location containing infringing material or activity by using information location tools (including a directory, index, reference, pointer or hypertext link), provided the Service Provider does not have actual knowledge that the material is infringing; is not aware of facts or circumstances from which infringing activity is apparent; does not receive a financial benefit directly attributable to any infringing activity for which it has the right and ability to control; and, if properly noticed of the infringing activity by the copyright holder or its authorized agent, or otherwise obtaining knowledge or awareness of the infringement, responds expeditiously to remove or disable access to the infringing material.³⁷⁶⁰ Section 512(d) does not mention framing as an example of an information location tool to which the safe harbor applies. Thus, although framing is accomplished by linking, it is unclear whether framing would fall within the safe harbor.³⁷⁶¹

The Service Provider can become aware of infringing activity either by notice from the copyright holder (or its authorized agent) or by virtue of other facts or circumstances of which it becomes aware. The same issues of knowledge that were discussed above with respect to the safe harbor of Section 512(c) apply also to the safe harbor of Section 512(d). Specifically, absent direct notice from the copyright holder or its agent, the standard of awareness of infringing activity appears by its terms to require more knowledge on the part of the Service Provider than

³⁷⁶⁰ Section 512(d) provides: “A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider –

(1)(A) does not have actual knowledge that the material or activity is infringing;

(B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link.”

³⁷⁶¹ Ballon & Kupferschmid, supra note 2969, at 8.

a “should have known” (or reason to know) standard – it requires that the Service Provider have actual awareness of facts from which infringing activity is apparent. As noted in the discussion of Section 512(c) above, the legislative history describes the standard of awareness as a “red flag” test.

a. The Napster Case

The first case to adjudicate the safe harbor under Section 512(d) was the Napster case, discussed extensively in Section III.C.2(c)(1) above. In that case, Napster asserted that the index it maintained on its servers of MP3 files available on the hard drives of its users constituted an information location tool, and that to the extent the plaintiffs’ infringement claims were based on the operation of that index, Napster was entitled to the safe harbor of Section 512(d). The district court, with only a very terse analysis contained entirely in a footnote, ruled that Napster was not entitled to the safe harbor because (i) it had constructive knowledge of infringing activity on its system (thereby failing to satisfy the requirement of Section 512(d)(1)(B))³⁷⁶² and (ii) “Defendant has failed to persuade this court that subsection 512(d) shelters contributory infringers.”³⁷⁶³

On appeal, the Ninth Circuit reversed this ruling of the district court. The Ninth Circuit noted that the district court’s ruling that the safe harbor would never apply to a Service Provider that might otherwise be liable as a contributory infringer was contrary to the legislative history of the DMCA.³⁷⁶⁴ The Ninth Circuit further stated, “We do not agree that Napster’s potential liability for contributory and vicarious infringement renders the Digital Millennium Copyright Act inapplicable per se. We instead recognize that this issue will be more fully developed at trial. At

³⁷⁶² The district court appears to have misapplied Section 512(d)(1)(B). Because Napster had constructive knowledge of infringing activity, and because Section 512(d)(1)(B) requires that the Service Provider be “not aware of facts or circumstances from which infringing activity is apparent,” the district court reasoned that Napster could not qualify for the safe harbor of Section 512(d). However, Section 512(d)(1) contains three prongs, which are stated in the disjunctive, not the conjunctive. Specifically, Section 512(d)(1) requires that the Service Provider have no actual knowledge of infringing material or activity (clause (A)), no awareness of facts or circumstances from which infringing activity is apparent (clause (B)), or “upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material” (clause (C)). Thus, even if a Service Provider has actual or constructive knowledge of infringing activity, so long as the Service Provider acts expeditiously to remove or disable access to the allegedly infringing material upon obtaining such knowledge, the safe harbor is still available. Napster asserted that in every instance in which it had obtained knowledge of infringing activity, it had acted expeditiously to block the account of the user who was allegedly sharing infringing material. Napster’s PI Opp. Br., supra note 2163, at 33.

³⁷⁶³ A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 919 n. 24 (N.D. Cal. 2000).

³⁷⁶⁴ A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025 (9th Cir. 2001) (quoting S. Rep. 105-90, at 40 (1998), which stated: “The limitations in subsections (a) through (d) protect qualifying service providers from liability for all monetary relief for direct, vicarious, and contributory infringement.”). This sentence from the legislative history was also quoted in a discussion of the scope of the DMCA safe harbors by the court in its opinion in In re Verizon Internet Services, Inc., 65 U.S.P.Q.2d 1574 (D.D.C. 2003). The court also stated, in the context of ruling on the scope of the subpoena power under Section 512(h) of the DMCA, that “in exchange for complying with subpoenas under subsection (h), service providers receive liability protection from any copyright infringement – direct or vicarious – by their users.” Id. at 1581 n.6.

this stage of the litigation, plaintiffs raise serious questions regarding Napster’s ability to obtain shelter under § 512, and plaintiffs also demonstrate that the balance of hardships tips in their favor.”³⁷⁶⁵

The Ninth Circuit noted that the following questions would have to be resolved at trial concerning whether Napster was entitled to the safe harbor of Section 512(d): “(1) whether Napster is an Internet service provider as defined by 17 U.S.C. § 512(d); (2) whether copyright owners must give a service provider ‘official’ notice of infringing activity in order for it to have knowledge or awareness of infringing activity on its system; and (3) whether Napster complies with § 512(i), which requires a service provider to timely establish a detailed copyright compliance policy.”³⁷⁶⁶

b. Perfect 10 v. Cybernet Ventures

The second case to adjudicate the Section 512(d) safe harbor was the case of Perfect 10, Inc. v. Cybernet Ventures, Inc.³⁷⁶⁷ As discussed in Section III.C.6(b)(1)(iii)d. above, the court concluded that the defendant Cybernet was not entitled to any of the Section 512 safe harbors because it had failed to satisfy the predicate requirements of Section 512(i). Nevertheless, the court, in a one sentence ruling also concluded that there was “a residual chance that Cybernet will qualify for 17 U.S.C. § 512(d)’s safe harbor for search engines, but not links.”³⁷⁶⁸ Because the court did not elaborate further, it is difficult to understand why the court reached this conclusion, particularly in view of its rulings with respect to Sections 512(i) and 512(c).

c. The MP3Board Case

Issues relating to the Section 512(d) safe harbor, and particularly its attendant notice requirements, arose in the case of Arista Records, Inc. v. MP3Board, Inc.,³⁷⁶⁹ and are discussed below in Section III.D.8.

d. The Aimster/Madster Lawsuits

The facts of the Aimster/Madster lawsuits are set forth in Section III.C.2(c)(3) above. In that case, Aimster asserted the Section 512(d) safe harbor. As discussed in Section III.C.6(b)(1)(i).c above, the district court concluded that Aimster was not entitled to any of the DMCA safe harbors because of its failure to satisfy the Section 512(i) predicate with respect to implementation of a policy to terminate repeat infringers on its system. In addition, the court

³⁷⁶⁵ Napster, 239 F.3d at 1025.

³⁷⁶⁶ Id. The bases for the district court’s doubts about whether Napster satisfied Section 512(i) are discussed in Section C.5(b)(1)(i)a. above with respect to the court’s ruling on whether Napster was entitled to the safe harbor of Section 512(a).

³⁷⁶⁷ 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

³⁷⁶⁸ Id. at 1182.

³⁷⁶⁹ 2002 U.S. Dist. LEXIS (S.D.N.Y. 2002).

held that Aimster had not satisfied the specific conditions of Section 512(d) because it had actual and constructive knowledge of the infringing activity for the same reasons that it had such knowledge for purposes of common law contributory liability (see the discussion in Section III.C.2(c)(3) above), and there was no evidence that Aimster had taken steps to remove or disable access to infringing material.³⁷⁷⁰ In addition, Aimster received a financial benefit directly attributable to the infringing activity and had the right and ability to control the infringing activity, again for the same reasons that it had such financial benefit and right and ability to control for purposes of common law vicarious liability (see the discussion in Section III.C.3(e) above).³⁷⁷¹ As discussed in Section III.C.6(b)(1)(i).c, on appeal the Seventh Circuit affirmed the ruling that the safe harbors were not available to Aimster because of failure to comply with Section 512(i).³⁷⁷²

e. The Diebold Lawsuit

Diebold was the manufacturer of electronic voting systems that contained a number of flaws. A series of internal Diebold emails acknowledging the flaws were published on the Internet. Diebold sent out dozens of cease and desist letters under the DMCA to websites linking to or publishing the Diebold emails, demanding that the materials, or links to the materials, be removed. The Electronic Frontier Foundation filed suit against Diebold on behalf of one of the ISPs and a news website publisher, arguing that linking to or publishing the materials was a fair use in order to comment on the reliability of electronic voting.³⁷⁷³ On Nov. 4, 2003, the court ordered Diebold to show why a preliminary injunction should not be issued to prevent Diebold from threatening to sue ISPs. In Dec. 2003, the court dismissed the plaintiffs' motion for the preliminary injunction as moot, after Diebold represented that it no longer demanded that the plaintiffs or any other party cease and desist using Diebold's email archive for noncommercial critical purposes. Diebold also agreed that it would retract all outstanding DMCA safe harbor notifications to ISPs concerning the email archive and would not issue such notifications to any party in any jurisdiction in the future.³⁷⁷⁴

In a subsequent action, one of the ISPs and two individual Swarthmore students who originally posted the Diebold emails on various websites sued Diebold, among other things, to recover damages and attorneys' fees under Section 512(f) of the DMCA on the ground that

³⁷⁷⁰ In re Aimster Copyright Litigation, 252 F. Supp. 2d 634, 661 (N.D. Ill. 2002).

³⁷⁷¹ Id.

³⁷⁷² In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003), cert. denied, 124 S. Ct. 1069 (2004).

³⁷⁷³ "ISP Rejects Diebold Copyright Claims Against News Website," available as of Jan. 17, 2004 at www.eff.org/Legal/ISP_liability/20031016_eff_pr.php. The suit, Online Policy Group v. Diebold, Inc., was filed in federal court in San Jose.

³⁷⁷⁴ "Electronic Voting Firm Drops DMCA, Copyright Charges Against ISPs," *Mealey's Litigation Report: Intellectual Property* (Dec. 15, 2003) 13-14.

Diebold's claims of copyright infringement were based on knowing material misrepresentations.³⁷⁷⁵ Section 512(f) of the DMCA provides:

Any person who knowingly materially misrepresents under this section –

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification,

shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

In adjudicating the plaintiff's Section 512(f) claim, the court first had to determine the validity of Diebold's claims that publication of its email archive constituted copyright infringement. The court concluded that publication of at least some of the email archive constituted fair use and was therefore not infringing. With respect to the purpose of the use, the court noted that discussion of problems associated with Diebold's electronic voting machines was clearly in the public interest. Moreover, Diebold had identified no specific commercial purpose or interest affected by publication of the archive, and there was no evidence that Diebold itself had intended to or could profit from such content. Finally, the plaintiffs' use of the material was transformative, in that they used the email archive to support criticism that was in the public interest, not to develop electronic voting technology.³⁷⁷⁶ Accordingly, the court ruled that "there is no genuine issue of material fact that Diebold, through its use of the DMCA, sought to and did in fact suppress publication of content that is not subject to copyright protection [because of the fair use doctrine.]"³⁷⁷⁷

The court then turned to whether Diebold knowingly materially misrepresented that publication of the email archive constituted copyright infringement. The parties disputed the meaning of the phrase "knowingly materially misrepresents." The plaintiffs argued that a preliminary injunction standard should be applied – that the court should conclude that Diebold violated Section 512(f) if it did not have a "likelihood of success" on the merits of the a copyright infringement claim when it sent the DMCA letters. Diebold contended that the court should apply a type of Federal Rule of Civil Procedure 11 standard and thus conclude that Diebold did not violation Section 512(f) unless sending the DMCA letters was "frivolous."³⁷⁷⁸

³⁷⁷⁵ Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195, 1198 (N.D. Cal. 2004).

³⁷⁷⁶ Id. at 1203.

³⁷⁷⁷ Id.

³⁷⁷⁸ Id. at 1204.

Acknowledging that it was facing an issue of first impression, the court concluded that neither proposed standard was appropriate. A requirement that a party have an objectively measured likelihood of success on the merits in order to assert claims of copyright infringement would impermissibly chill the rights of copyright owners. On the other hand, in requiring a showing of “knowing material misrepresentation,” Congress explicitly adopted a standard from Rule 11, which contains a variety of other requirements that are not necessarily coextensive with those of Section 512(f).³⁷⁷⁹

Instead, the court concluded that the statutory language was sufficient clear on its fact and does not require importation of standards from other legal contexts. Citing Black’s Law Dictionary, the court held that “knowingly” means that a party actually knew, should have known if it acted with reasonable care or diligence, or would have had no substantial doubt had it been acting in good faith, that it was making misrepresentations. “Material” means that the misrepresentation affects the ISP’s response to a DMCA letter.³⁷⁸⁰

Under this standard, the court concluded as a matter of law that Diebold knowingly materially misrepresented that the plaintiffs infringed Diebold’s copyright interest, at least with respect to the portions of the email archive clearly subject to the fair use exception:

No reasonable copyright holder could have believed that the portions of the email archive discussing possible technical problems with Diebold’s voting machines were protected by copyright, and there is no genuine issue of fact that Diebold knew – and indeed that it specifically intended – that its letters to OPG and Swarthmore would result in prevention of publication of that content. The misrepresentations were material in that they resulted in removal of the content from websites and the initiation of the present lawsuit. The fact that Diebold never actually brought suit against any alleged infringer suggests strongly that Diebold sought to use the DMCA’s safe harbor provisions – which were designed to protect ISPs, not copyright holders – as a sword to suppress publication of embarrassing content rather than as a shield to protect its intellectual property.³⁷⁸¹

³⁷⁷⁹ Id.

³⁷⁸⁰ Id.

³⁷⁸¹ Id. at 1204-05. The court also held that the plaintiff’s claim that Diebold, through its inappropriate use of the DMCA, had interfered with their contractual relations with their respective ISPs, was preempted. “Even if a copyright holder does not intend to cause anything other than the removal of allegedly infringing material, compliance with the DMCA’s procedures nonetheless may result in disruption of a contractual relationship: by sending a letter, the copyright holder can effectuate the disruption of ISP service to clients. If adherence to the DMCA’s provisions simultaneously subjects the copyright holder to state tort liability, there is an irreconcilable conflict between state and federal law. Id. at 1205-06.

Two weeks after the court rendered its judgment, Diebold agreed to settle the lawsuit by paying \$125,000 in damages and fees to the plaintiffs.³⁷⁸²

f. Perfect 10 v. CCBill

The facts of this case are set forth in Section III.C.6(b)(1)(i)d. above. In that case, the defendant Internet Key, an age verification service for adult content websites, filed a motion for summary judgment under the Section 512(d) safe harbor. Perfect 10 argued that Internet Key was not entitled to the safe harbor because it was not an information location tool, it had actual knowledge of infringements, and it was aware of facts or circumstances from which infringing activity was apparent.³⁷⁸³

With respect to the issue of whether Internet Key was an information location tool, the court rejected Perfect 10's argument that Section 512(d) is limited to OSPs like Google and Yahoo! that provide links to millions of web sites and that do not have contractual relationships with their affiliate web sites. Instead, Section 512(d) refers to OSPs who refer or link users to an online location containing infringing material or activity by using a directory, index, reference, point, hypertext link or the like. The court concluded that Internet Key's sexkey.com web site provided that function and was therefore covered by Section 512(d).³⁷⁸⁴

With respect to the knowledge element, Perfect 10 argued that Internet Key should have known that there were copyright infringements on its clients' web sites because of the disclaimers on some of those web sites, which generally claimed that the copyrighted images were in the public domain or that the webmaster was posting the images for newsworthy purposes. The court ruled that these disclaimers were not sufficient to raise a "red flag" of copyright infringement, which is the standard of constructive knowledge under Sections 512(c) and 512(d).³⁷⁸⁵

Turning to the issue of control, the court ruled, citing Costar Group, Inc. v. Loopnet, Inc.³⁷⁸⁶ and Perfect 10 v. Cybernet Ventures, Inc.,³⁷⁸⁷ that the mere ability to disconnect the webmasters' access to Internet Key's service was not sufficient under the DMCA to demonstrate a right and ability to control the infringing activity. Because no other control had been shown, Internet Key was entitled to summary judgment under the Section 512(d) safe harbor.³⁷⁸⁸

³⁷⁸² "Diebold Settles Landmark DMCA Suit in Dispute Over Voting Machines," *IP Law Bulletin* (Oct. 15, 2004), available as of Oct. 18, 2004 at www.iplawbulletin.com/cgi-bin/absolutenm/anmviewer.asp?a=2381&z=18.

³⁷⁸³ Perfect 10, Inc. v. CCBill, 340 F. Supp. 2d 1077, 1097-98 (C.D. Cal. 2004).

³⁷⁸⁴ Id.

³⁷⁸⁵ Id. at 1098.

³⁷⁸⁶ 164 F. Supp. 2d 688, 704 (D. Md. 2001), aff'd, 373 F.3d 544 (4th Cir. 2004).

³⁷⁸⁷ 213 F. Supp. 2d 1146, 1181 (C.D. Cal. 2002).

³⁷⁸⁸ Perfect 10 v. CCBill, 340 F. Supp. 2d at 1098.

The parties filed an appeal of the rulings in this case with respect to CCBill and CWIE, although not with respect to Internet Key. On appeal, CCBill argued that it should be entitled to the immunity of Section 512(d) because, after processing a consumer's credit card and issuing a password granting access to a client website, it displayed a hyperlink so that the user could access the client website. The Ninth Circuit rejected this argument, noting that, even if the displayed hyperlink could be viewed as an information location tool, Section 512(d) provides a safe harbor only for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or activity. Perfect 10 had not claimed that CCBill infringed its copyrights by providing a hyperlink, but rather through CCBill's performance of other business services for the infringing websites. Accordingly, even if CCBill's provision of a hyperlink were immune under Section 512(d), CCBill could not receive blanket immunity under Section 512(d) for its other services.³⁷⁸⁹

g. Columbia Pictures v. Fung

In Columbia Pictures Industries, Inc. v. Fung,³⁷⁹⁰ the defendants operated BitTorrent sites through which users could search indexes for dot-torrent files pointing to infringing movies and other content. The district court found the defendants liable for inducement of infringement and rejected assertion of a safe harbor under Section 512(d). The plaintiffs had established that the defendants had reason to know of their users' infringing activities (plaintiffs' expert testified that approximately 95% of downloads occurring through the defendants' sites were downloads of infringing content) and therefore the defendants had failed to establish the first requirement of the Section 512(d) safe harbor that they were not aware of facts or circumstances from which infringing activity was apparent.³⁷⁹¹ The court found that the defendants also had adequate knowledge of infringing activity under the "red flag" test to have a duty to act to removing links to infringing content. The defendants had not introduced any evidence that they acted expeditiously to remove or disable access to infringing material. In addition, the court held the defendants had failed to raise a triable issue of fact regarding the second requirement of the Section 512(d) safe harbor, because they had received a financial benefit directly attributable to the infringing activity, which acted as a major draw for users to the site and from which the defendants derived revenue, and they had the right and ability to control such activity.³⁷⁹²

Finally, the court ruled that, as a general proposition, "inducement liability and the Digital Millennium Copyright Act safe harbors are inherently contradictory. Inducement liability is based on active bad faith conduct aimed at promoting infringement; the statutory safe harbors

³⁷⁸⁹ Perfect 10, Inc. v. CCBill LLC, 481 F.3d 751, 765-66 (9th Cir.), cert. denied, 552 U.S. 1062 (2007).

³⁷⁹⁰ 2009 U.S. Dist. LEXIS 122661 (C.D. Cal. Dec. 21, 2009), aff'd, 710 F.3d 1020 (9th Cir. 2013).

³⁷⁹¹ Id. at *17 & *61.

³⁷⁹² Id. at *55, *61-66, & *62 n.27.

are based on passive good faith conduct aimed at operating a legitimate internet business. Here ... Defendants are liable for inducement. There is no safe harbor for such conduct.”³⁷⁹³

On appeal, the Ninth Circuit affirmed that the defendants did not qualify for the Section 512(d) safe harbor, but on different grounds. Specifically, the court held that the defendants did not qualify for the Section 512(d) safe harbor under the knowledge, financial benefit, and right to control prongs of Section 512(d) for the same reasons those prongs applied to preclude safe harbor protection under Section 512(c), as discussed in detail in Section III.C.6(b)(1)(iii).v above.³⁷⁹⁴

h. Perfect 10 v. Google

The rulings of this case with respect to the Section 512(d) safe harbor are discussed in Section III.C.6(b)(1)(ii) above.

i. Perfect 10 v. Yandex

In Perfect 10, Inc. v. Yandex,³⁷⁹⁵ Yandex offered a broad range of search functions over the Internet. Perfect 10 sent hundreds of DMCA takedown notices to Yandex requesting that it remove links to thousands of allegedly infringing images. Perfect 10 moved for partial summary judgment that three sample DMCA notices were substantially compliant with the notice requirements of Section 512(c)(3)(A) and (d)(3) and that Yandex was ineligible for any DMCA safe harbor defense during the period when it had no DMCA agent registered with the Copyright Office.³⁷⁹⁶

The court granted partial summary judgment with respect to sample notice 1, finding that it complied with the notice requirements, but denied summary judgment as to sample notices 2 and 3. Sample notice 1 consisted of a PDF file that began with a short DMCA notice letter that described the contents of the DMCA notice itself and requested that the images be taken down. The notice letter was followed by several pages of screen shots from Yandex’s own image search web sites. The screen shots showed the allegedly copyrighted images in Yandex’s search results along with corresponding links to the party directly hosting the content. In many instances the links to the third party sites were truncated, but it was possible to copy the whole link by right clicking on the image in the file. At the end of each sample notice was a single screen shot from Perfect 10’s own website that included the allegedly copyrighted images in a four-by-four grid of images. Yandex argued that sample notice 1 was deficient because it failed to sufficiently identify the location of the allegedly infringing materials by virtue of the fact that some of the links in the screen shots were truncated. The court rejected this argument, noting that the truncated links were generated as part of Yandex’s own search results. The sample

³⁷⁹³ Id. at *67-68.

³⁷⁹⁴ Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1047 (9th Cir. 2013).

³⁷⁹⁵ 2013 U.S. Dist. LEXIS 65802 (N.D. Cal. May 7, 2013).

³⁷⁹⁶ Id. at *2-4.

notice used the screen shots to prove that the images were linked from Yandex’s site, not to identify the location of the allegedly infringing content. Because the full links were available by clicking or right clicking on the images listed in the search results, sample notice 1 was adequate under the requirements of the DMCA.³⁷⁹⁷

The court did not consider sample notice 2 because it had not been shown to implicate domestic infringement. Yandex challenged the adequacy of sample notice 3 on the ground that in one instance the authorized copy and the alleged infringements were not the identical work. The court rejected this, noting there is no express requirement in the statute that a DMCA notice include an exact, authorized copy of an allegedly infringing work, or even *any* authorized copy of such work. Nevertheless, the court ruled that the voluntary inclusion of an incorrect version of the original work raised questions as to how the notice would have been understood by the recipient, a factual question that the jury must resolve.³⁷⁹⁸

Perfect 10 also sought partial summary judgment that the compliant sample notices necessarily conferred actual knowledge of infringement for the purposes of its contributory liability claim. The court rejected this, pointing to Ninth Circuit authority that a DMCA-compliant notice provides only a claim of infringement, and is not necessarily sufficient by itself to establish actual or red flag knowledge. There was therefore a genuine issue of material fact regarding whether Yandex had actual knowledge of contributory infringement, and the court denied Perfect 10 summary judgment on the point.³⁷⁹⁹

Finally, the court granted Perfect 10 partial summary judgment that Yandex was ineligible for the DMCA safe harbor during the period in which it had no registered DMCA agent. The court rejected Yandex’s argument that Section 512(c)(2) does not require that its agent be registered with the Copyright Office, only that it have an agent, on the ground that Congress intended for the courts to enforce only substantial compliance with the DMCA’s safe harbor requirements. The court noted that the phrase “substantially the following information” in the statutory provision requiring registration of an agent modifies the ensuing subparagraphs that list types of contact information for an agent, and does not excuse a failure to provide the Copyright Office with any information at all.³⁸⁰⁰

(2) General Requirements for Limitations of Liability

In addition to meeting the requirements of one of the specific safe harbors, to be eligible for the limitations of liability, under Section 512(i) the Service Provider must adopt, reasonably implement, and inform subscribers of a policy for the termination in appropriate circumstances of subscribers who are repeat infringers, and must not interfere with standard technical measures used by copyright owners to identify or protect copyrighted works that have been

³⁷⁹⁷ *Id.* at *10-15.

³⁷⁹⁸ *Id.* at *15-17.

³⁷⁹⁹ *Id.* at *17-19.

³⁸⁰⁰ *Id.* at *19-21.

developed “pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process,” are available to any person on reasonable and nondiscriminatory terms, and do not impose substantial costs or burdens on Service Providers or their systems.

Most commercial Service Providers have a policy with respect to use of the service by subscribers. The policy may be posted on the Service Provider’s website, contained in the subscription agreement, or both. Operators of corporate intranets will likewise want to post a policy on the intranet itself, and may wish to update employee handbooks or policy manuals to incorporate the policy statements required to take advantage of the safe harbors. All Service Providers should reasonably document their efforts to enforce their policies.

(i) What Constitutes a “Standard Technical Measure”

a. Perfect 10 v. CCBill

As discussed in Section III.C.6(b)(1)(i).d above, Perfect 10 argued in this case that the defendants failed the predicate condition of Section 512(i)(1)(B) of not interfering with standard technical measure used to identify or protect copyrighted works, by blocking Perfect 10’s access to CCBill affiliated websites in order to prevent Perfect 10 from discovering whether those websites infringed Perfect 10’s copyrights. The Ninth Circuit found two disputed facts at issue for purposes of summary judgment. First, the court was unable to determine on the record whether accessing websites is a standard technical measure that was developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process, as required by Section 512(i)(2)(A). Second, even if it were a standard technical measure, CCBill claimed it blocked Perfect 10’s credit card only because Perfect 10 had previously reversed charges for subscriptions. Perfect 10 insisted CCBill did so in order to prevent Perfect 10 from identifying infringing content. If CCBill were correct, Perfect 10’s method of identifying infringement – forcing CCBill to pay the fines and fees associated with chargebacks – might well impose a substantial cost on CCBill. If not, CCBill might well have interfered with Perfect 10’s efforts to police the websites in question for possible infringements. Accordingly, the court remanded to the district court for determinations on whether access to a website is a standard technical measure, and if so, whether CCBill’s refusal to process Perfect 10’s transactions interfered with that measure for identifying infringement.³⁸⁰¹

b. Wolk v. Kodak Imaging Networks

As discussed in Section III.C.6(b)(1)(iii).q above, the court in this case rejected the plaintiff’s argument that Photobucket failed to accommodate standard technical measures because it afforded its users computer tools that allowed users to obliterate, hide or crop out the copyright watermarks on images uploaded. The court noted that the plaintiff had not suggested that Photobucket advised or encouraged its users to use the photo editing tools to circumvent the copyright notice. In any event, the court found the fact that the watermarks

³⁸⁰¹ Perfect 10, Inc. v. CCBill LLC, 481 F.3d 751, 764 (9th Cir.), cert. denied, 552 U.S. 1062 (2007).

appeared on content on the site suggested that Photobucket did, in fact, accommodate standard technical measures. Although the plaintiff argued that the editing software interfered with standard technical measures, the court noted that it was not Photobucket, but rather users, who would use the editing tools to attempt to circumvent copyright protection measures that were already on the site. Accordingly, the editing tools did not disqualify Photobucket from safe harbor eligibility.³⁸⁰²

c. Obodai v. Demand Media

As discussed in Section III.C.6(b)(1)(iii).u above, the court noted that an example of a party's failure to comply with standard technical measures may include conduct that advises or encourages users to conceal a work's copyrighted status. To the extent the plaintiff in this case contested that issue, the plaintiff argued that the defendant distributed copyrighted texts and entered into some form of a distribution agreement. The court noted that, while probative of other relevant considerations, these facts were not evidence of interference with standard technical measures under the DMCA.³⁸⁰³

d. Capitol Records v. Vimeo

As discussed in Section III.C.6(b)(1)(iii).y. Above, although the plaintiffs in this case did not expressly argue that Vimeo failed to meet the requirement that it not interfere with standard technical measures used by copyright owners to identify or protect copyrighted works, the court noted that the plaintiffs did claim that Vimeo's privacy settings prevented copyright owners from collecting information needed to issue a takedown notice. Even if true, the court found such fact insufficient to demonstrate failure to meet the non-interference with standard technical measures requirement. Apart from the fact that the plaintiffs had not identified a standard technical measure that comported with the statute's definition, the court held that privacy settings do not constitute interference with standard technical measures.³⁸⁰⁴

e. BWP Media v. Polyvore

The facts and rulings of this case are set forth in Section III.C.1(g) above. Although the court made no ruling with respect to what constitutes a "standard technical measure," the court did note that the plaintiffs had raised an interesting legal issue as to whether the preservation of metadata, which allowed the plaintiffs to identify their photographs on other web sites and which Polyvore purportedly deleted when photos were uploaded to its web site by users, was a standard technical measure that Polyvore must accommodate and not interfere with in order to invoke the DMCA safe harbor provisions. The court concluded that it need not address the issue

³⁸⁰² Wolk v. Kodak Imaging Networks, Inc., 840 F. Supp. 2d 724, 744-45 (S.D.N.Y. 2012), aff'd sub nom. Wolk v. Photobucket, Inc., 569 Fed. Appx. 51 (2d Cir. 2014) (summary order).

³⁸⁰³ Obodai v. Demand Media, Inc., 2012 U.S. Dist. LEXIS 83109 at *13-14 (S.D.N.Y. June 13, 2012), aff'd, 2013 U.S. App. LEXIS 10734 (2d Cir. May 29, 2013).

³⁸⁰⁴ Capitol Records, LLC v. Vimeo, LLC, 972 F. Supp. 2d 500, 517 (S.D.N.Y. 2013), aff'd in part & vacated and remanded in part on other grounds, 2016 U.S. App. LEXIS 10884 (June 16, 2016).

because the plaintiffs had not met their initial burden to present proof of any volitional conduct on behalf of Polyvore, and they were therefore unable to establish a prima facie case of copyright infringement to which a DMCA safe harbor might be a defense.³⁸⁰⁵

(3) Special Provisions for Nonprofit Educational Institutions

Section 512(e) contains an additional liability limitation for nonprofit educational institutions. According to the Conference Report, Congress recognized that university environments are unique, and a university might otherwise fail to qualify for the safe harbors simply because the knowledge or actions of one of its employees might be imputed to the university under basic principles of respondent superior and agency law. Based upon principles of academic freedom and independence, Congress believed that in certain circumstances it would be inappropriate for actions online of faculty members and graduate students to be imputed to the university to prevent it from being eligible for the safe harbors.

Accordingly, Section 512(e) provides that online infringing actions of faculty members or graduate student employees that occur when they are “performing a teaching or research function” will not be attributed to the university in its capacity as their employer, and the university will therefore not be charged with such faculty member’s or graduate student’s knowledge or awareness of his or her infringing activities, if (i) the infringing activities do not involve the provision of online access to instructional materials that are or were required or recommended, within the preceding three-year period, for a course taught at the university by such faculty member or graduate student; (ii) the university has not, within the preceding three-year period, received more than two notifications of claimed infringement by such faculty member or graduate student; and (iii) the university provides all users of its system with informational materials that accurately describe and promote compliance with U.S. copyright law.

(4) Filing of False DMCA Notices – Section 512(f)

Section 512(f) of the DMCA provides:

Any person who knowingly materially misrepresents under this section –

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification,

shall be liable for any damages, including costs and attorneys’ fees, incurred by the alleged infringer, by any copyright owner or copyright owner’s authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the

³⁸⁰⁵ BWP Media USA Inc. v. Polyvore, Inc., 2016 U.S. Dist. LEXIS 92121 at *2 (S.D.N.Y. July 15, 2016), aff’d in part & rev’d in part, 922 F.3d 42 (9th Cir. 2019).

material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

In Twelve Inches Around Corp. v. Cisco Sys., the court ruled that Section 512(f) does not apply to misrepresentations of trademark infringement on a website.³⁸⁰⁶ The Eleventh Circuit reached the same conclusion in Mandala v. Tire Stickers, LLC.³⁸⁰⁷

(i) Rossi v. MPAA

The first case to adjudicate the scope of Section 512(f) was that of Rossi v. MPAA.³⁸⁰⁸ A discussion of the Ninth Circuit's rulings with respect to Section 512(f) may be found in Section III.C.6(b)(1)(iii).g above.

(ii) Online Policy Group v. Diebold, Inc.

The second case to adjudicate the scope of Section 512(f) was that of Online Policy Group v. Diebold, Inc.³⁸⁰⁹ A discussion of the court's rulings with respect to Section 512(f) may be found in Section III.C.6(b)(1)(iv).e above.

(iii) Dudnikov v. MGA Entertainment

In Dudnikov v. MGA Entertainment, Inc.,³⁸¹⁰ the court ruled that a request by the defendant to eBay to take down the auction of a fleece hat with a Bratz appliqué on it did not give rise to a claim under Section 512(f) because the defendant acted in a good faith belief that the sale of the hat infringed its copyright and trademark rights and the plaintiffs had failed to satisfy their burden of demonstrating that the defendant knowingly and materially misrepresented that the plaintiffs' auction was infringing. The court rejected the plaintiffs' argument that a higher standard of good faith should be applied just because the defendant's agent who issued the takedown notice was a lawyer trained in intellectual property law.³⁸¹¹

(iv) Novotny v. Chapman

In Novotny v. Chapman,³⁸¹² the defendant made instructional videos in which he demonstrated a particular method of cutting women's hair. In 2002, he entered into an agreement with the plaintiffs in which he would deliver originals of his video to the plaintiffs, who would then convert them into digital format and publish and sell them on their Web site as

³⁸⁰⁶ 2009 U.S. Dist. LEXIS 34966 at *6-9 (S.D.N.Y. Mar. 12, 2009).

³⁸⁰⁷ 2020 U.S. App. LEXIS 31016 at *11-12 (11th Cir. Sept. 30, 2020).

³⁸⁰⁸ 391 F.3d 1000 (9th Cir. 2004).

³⁸⁰⁹ 337 F. Supp. 2d 1195 (N.D. Cal. 2004).

³⁸¹⁰ 410 F. Supp. 2d 1010 (D. Colo. 2005).

³⁸¹¹ *Id.* at 1012-13.

³⁸¹² 2006 U.S. Dist. LEXIS 55471 (W.D.N.C. 2006).

downloadable streaming media clips. In October of 2004, as sales of the videos began to wane, the defendant sent the plaintiffs an email requesting that they remove his videos from their Web site. After the plaintiffs refused to do so, the defendant filed notices of copyright infringement under the DMCA with the plaintiffs' Internet service providers, alleging that material on the plaintiffs' Web site was infringing on the defendant's copyrights in his videos. Both the Internet service providers and the Paypal service, which processed payments for the plaintiffs' Web site, suspended the plaintiffs' access to their accounts. In response, the plaintiffs removed the videos from their Web site. The defendant thereafter filed no further DMCA notices.³⁸¹³

The plaintiffs accused the defendant of violating Section 512(f) by filing bad faith complaints of copyright infringement with the plaintiffs' Internet service providers and others, with the intent that such complaints would result in the suspension of the plaintiffs' Internet services and accounts, and asked the court to enjoin the defendant from filing any more such complaints.³⁸¹⁴ The court denied the injunction on the ground that the injury the plaintiffs sought to avoid – the damage to reputation and business interests caused by the defendant's filing of improper DMCA complaints with the plaintiffs' service providers – was not likely to recur since the plaintiffs neither were posting the videos at issue on their Web site, nor had they cited any interest in re-posting the videos before the underlying legal issues were resolved.³⁸¹⁵

(v) BioSafe-One, Inc. v. Hawks

In BioSafe-One, Inc. v. Hawks,³⁸¹⁶ the defendants inadvertently copied some textual materials from the plaintiffs' web site into the defendants' web site. Upon discovering the copying, the defendants removed the copied materials. After removal of the copied materials, but before the plaintiffs knew that the copied materials had been removed, the plaintiffs sent two DMCA notices to the OSPs hosting the defendants' web site. In both instances, the OSPs shut down the defendants' web site in response. The defendants claimed that the plaintiffs' notices under the DMCA violated Section 512(f) and sought an injunction preventing the plaintiffs from further interfering with their web site.³⁸¹⁷

The court ruled the defendants had failed to present sufficient evidence that the plaintiffs knowingly materially misrepresented to the OSPs that the defendants' web site was infringing. The plaintiffs had submitted ample evidence and testimony that they believed the defendants' web site violated their copyright when the DMCA notices were submitted. Accordingly, the court denied the defendants' claim under Section 512(f). However, the court granted a preliminary injunction barring the plaintiffs from sending additional DMCA notices in

³⁸¹³ Id. at *2-5.

³⁸¹⁴ Id. at *1.

³⁸¹⁵ Id. at *7-8.

³⁸¹⁶ 2007 U.S. Dist. LEXIS 88032 (S.D.N.Y. Nov. 29, 2007).

³⁸¹⁷ Id. at *1-3.

view of the fact that the court had ruled that the defendants' web site, after the copied materials had been removed, was not substantially similar to the plaintiffs' web site.³⁸¹⁸

(vi) **Lenz v. Universal Music Corp.**

The District Court Decisions

In Lenz v. Universal Music Corp.,³⁸¹⁹ Stephanie Lenz videotaped her toddler son dancing in the family's kitchen to the song titled "Let's Go Crazy" owned by the musician known as "Prince," and posted the video on YouTube.com. Universal sent a DMCA takedown notice to YouTube, which responded by removing the video from the site. Lenz sent YouTube a counter-notification under the DMCA, demanding that her video be re-posted because it did not infringe the plaintiff's copyrights, and the video was then re-posted by YouTube. Lenz then filed an action against Universal under Section 512(f) seeking redress for Universal's alleged misuse of the DMCA takedown process, arguing that her posting was a self-evident non-infringing fair use.³⁸²⁰

The court rejected Lenz's claim. Citing the Rossi case discussed in subsection (i) above, the court ruled that Lenz must show a knowing misrepresentation on the part of the copyright owner in filing the takedown notice in order to establish liability under Section 512(f). The court noted that Universal had not conceded that the posting was a fair use, and Lenz had failed to allege facts from which a misrepresentation could be inferred or why her use of the song was a self-evident fair use. Accordingly, Lenz's claim was dismissed with leave to amend.³⁸²¹

Lenz then amended her complaint, alleging that Universal had issued the DMCA takedown notice only to appease Prince, the author of the song "Let's Go Crazy."³⁸²² Specifically, Lenz alleged that Universal issued its DMCA notice to YouTube at Prince's behest, based not on the particular characteristics of the video or any good faith belief that it actually infringed, but rather to appease him, as evidenced by an October 2007 statement to ABC News, in which Universal made the following comment:

Prince believes it is wrong for You-Tube, or any other user-generated site, to appropriate his music without his consent. That position has nothing to do with any particular video that uses his songs. It's simply a matter of principle. And legally, he has the right to have his music removed. We support him and this important principle. That's why, over the

³⁸¹⁸ Id. at *30-31.

³⁸¹⁹ 2008 U.S. Dist. LEXIS 44549 (N.D. Cal. Apr. 8, 2008) (Order Granting Defendants' Motion to Dismiss with Leave to Amend) (not for citation).

³⁸²⁰ Id. at *1-3.

³⁸²¹ Id. at *8-9.

³⁸²² Lenz v. Universal Music Corp., 572 F. Supp. 2d 1150, 1152 (N.D. Cal. 2008).

last few months, we have asked YouTube to remove thousands of different videos that use Prince music without his permission.³⁸²³

Universal moved to dismiss the case for failure to state a claim upon which relief could be granted. The issue raised by the motion, which the court found to be an issue of first impression, was whether the requirement of Section 512(c)(3)(A)(v) that a notice issued under Section 512(c) contain a statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law, requires a copyright owner to consider the fair use doctrine in formulating its good faith belief. Universal contended that Section 512(c)(3)(A)(v) does not require copyright owners to evaluate the question of fair use prior to sending a takedown notice because fair use is merely an *excused* infringement of copyright rather than a use *authorized* by the copyright owner or by law. Universal also contended that even if a copyright owner were required by the DMCA to evaluate fair use with respect to allegedly infringing material, any such duty would arise only *after* a copyright owner received a counter-notice and considered filing suit.³⁸²⁴

The court ruled that a copyright owner does have a duty to consider the applicability of the fair use doctrine before issuing a takedown notice:

An activity or behavior “authorized by law” is one permitted by law or not contrary to law. Though Congress did not expressly mention the fair use doctrine in the DMCA, the Copyright Act provides explicitly that “the fair use of a copyrighted work ... is not an infringement of copyright.” 17 U.S.C. § 107. Even if Universal is correct that fair use only *excuses* infringement, the fact remains that fair use is a lawful use of a copyright. Accordingly, in order for a copyright owner to proceed under the DMCA with “a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law,” the owner must evaluate whether the material makes fair use of the copyright. 17 U.S.C. § 512(c)(3)(A)(v). An allegation that a copyright owner acted in bad faith by issuing a takedown notice without proper consideration of the fair use doctrine thus is sufficient to state a misrepresentation claim pursuant to *Section 512(f)* of the DMCA.³⁸²⁵

The court addressed Universal’s concern that, because the question of whether a particular use of copyrighted material is fair is a fact-intensive inquiry, it would be difficult for copyright owners to predict whether a court eventually would rule in their favor. “[W]hile these concerns are understandable, their actual impact likely is overstated. Although there may be cases in which such considerations will arise, there are likely to be few in which a copyright owner’s determination that a particular use is not fair use will meet the requisite standard of

³⁸²³ *Id.* at 1152-53.

³⁸²⁴ *Id.* at 1153-54.

³⁸²⁵ *Id.* at 1154-55 (footnotes omitted).

subjective bad faith required to prevail in an action for misrepresentation under 17 U.S.C. § 512(f).”³⁸²⁶

The court then turned to whether the amended complaint contained sufficient allegations of bad faith and deliberate ignorance of fair use to survive the motion to dismiss. The court found that it did. The amended complaint alleged that Universal acted solely to satisfy Prince and his personal agenda and that its actions had nothing to do with any particular YouTube video that used his songs.³⁸²⁷ The court concluded, “Although the Court has considerable doubt that Lenz will be able to prove that Universal acted with the subjective bad faith required by *Rossi*, and following discovery her claims well may be appropriate for summary judgment, Lenz’s allegations are sufficient at the pleading stage.”³⁸²⁸

Finally, the court considered Universal’s allegation that the amended complaint failed to allege a compensable loss under the DMCA. The amended complaint alleged that Lenz had incurred injury in the form of the financial and personal expenses associated with responding to the claim of infringement and harm to her free speech rights, and that she had been intimidated into not posting a single video on YouTube since she received Universal’s takedown notice. At oral argument, Lenz’s counsel stated that while the damages incurred in preparing Lenz’s counter-notice could not be elaborated upon for reasons of privilege, Lenz did incur actual damages in reviewing counter-notice procedures, seeking the assistance of an attorney, and responding to the takedown notice. The court ruled that, though damages might be nominal and their exact nature yet to be determined, Lenz had adequately alleged cognizable injury under the DMCA to survive Universal’s motion to dismiss.³⁸²⁹

In a later opinion (designated not for publication) denying the defendants’ motion to certify the court’s order for interlocutory appeal, the court elaborated on its ruling a bit as follows: “The Court did not hold that every takedown notice must be preceded by a full fair use investigation. Rather, it recognized, as it has previously, that in a given case fair use may be so obvious that a copyright owner could not reasonably believe that actionable infringement was taking place. In such a case, which is likely to be extremely rare, the policy objectives of the DMCA are served by requiring copyright owners at least to form a subjective good faith belief that the ‘particular use is not a fair use’ before sending the takedown notice.”³⁸³⁰

Lenz then moved for partial summary judgment with respect to several affirmative defenses asserted by the defendants.³⁸³¹ The defendants’ third affirmative defense was that Lenz had suffered no damages cognizable under Section 512(f), which provides that a person

³⁸²⁶ Id. at 1155.

³⁸²⁷ Id. at 1156.

³⁸²⁸ Id.

³⁸²⁹ Id. at 1156-57.

³⁸³⁰ Lenz v. Universal Music Corp., 2008 U.S. Dist. LEXIS 91890 at *6-7 (N.D. Cal. Oct. 28, 2008) (citations omitted).

³⁸³¹ Lenz v. Universal Music Corp., 2010 U.S. Dist. LEXIS 16899 (N.D. Cal. Feb. 25, 2010).

who knowingly makes a material misrepresentation in a takedown notice or in a counternotice shall be liable for “any damages,” including costs and attorneys’ fees, incurred by one injured by the misrepresentation as the result of the service provider relying on the misrepresentation in removing the allegedly infringing materials or in replacing removed material. The parties disagreed about whether the statute recognizes only economic damages. The court ruled that the use of the phrase “any damages” suggested strong congressional intent that recovery be available for damages even if they do not amount to substantial economic damages.³⁸³² All the plaintiff need show is damages that were “proximately caused by the misrepresentation to the service provider and the service provider’s reliance on the misrepresentation.”³⁸³³ With respect to attorneys’ fees and costs, the court ruled that any fees incurred for work in responding to the takedown notice and prior to the institution of suit under Section 512(f) are recoverable, but recovery of any other costs and fees post institution of suit is governed by the usual standard under Section 505. Because there was no genuine issue of material fact as to whether Lenz incurred at least *some* damages as defined under the statute, the court granted Lenz’s motion for summary judgment as to Universal’s affirmative defense of no damages.³⁸³⁴

In a later opinion upon cross motions for summary judgment, the court had an opportunity to elaborate further on what consideration of fair use is required of a copyright holder before issuing a DMCA takedown notice. As an initial matter, the parties disputed whether the DMCA applied at all in the case. Universal contended that its takedown notice did not constitute a notification of claimed infringement under Section 512 at all, and thus any misrepresentations contained therein could not give rise to DMCA liability.³⁸³⁵ Universal based its argument on the fact that its takedown notice to YouTube stated: “In addition, our use of YouTube’s required notice form does not indicate we believe that the above referenced copyright infringement is within the scope of the Digital Millennium Copyright Act (‘DMCA’). Our use of this form, as required by YouTube, is meant to facilitate YouTube’s removal of the infringing material listed above and is not meant to suggest or imply that YouTube’s activities and services are within the scope of the DMCA safe harbor.”³⁸³⁶ The court rejected this argument, noting that YouTube’s Terms of Use stated that only DMCA notices should be sent to its Copyright Agent, and that any other communications should be directed to YouTube customer services at a specified URL. Universal had sent its takedown notice to YouTube’s Copyright Agent, and its form complied with the requirements of Section 512(c) for a proper DMCA notice. The court noted that Universal had not pointed to any authority suggesting that its subjective intent, as expressed in the language quoted above in its takedown notice, had any relevance to the legal adequacy of the takedown notice for purposes of the DMCA.³⁸³⁷

³⁸³² Id. at *20-26.

³⁸³³ Id. at *26 (emphasis removed).

³⁸³⁴ Id. at *29-30.

³⁸³⁵ Lenz v. Universal Music Corp., 2013 U.S. Dist. LEXIS 9799 at *7 (N.D. Cal. Jan. 24, 2013).

³⁸³⁶ Id. at *9.

³⁸³⁷ Id. at *7-10.

The court then elaborated on the relationship between the fair use doctrine and submission of a DMCA takedown notice. First, the court found sufficient evidence in the record to establish that Universal issued its takedown notice without considering fair use. The only person at Universal who reviewed YouTube videos for violations of Prince's copyrights testified that he put Lenz's video on the list for takedown because he recognized the song in the background immediately, the song was loud and played through the entire video, and the audio track included a voice asking the children whether they liked the music. He made no mention of fair use during his testimony and gave no indication that he considered fair use before deciding whether to place Lenz's video on the removal list. Universal also admitted in a request for admission that as of the date of the takedown notice, it had not instructed the employee to consider fair use during his review of YouTube videos.³⁸³⁸ The court stated:

While it agrees that requiring a copyright holder to engage in a full-blown fair use analysis prior to sending a DMCA takedown notice would be inconsistent with the remedial purposes of the statute, the Court disagrees that it is sufficient for a copyright holder to consider facts that might be relevant to a fair use analysis without making any effort to evaluate the significance of such facts in the context of the doctrine itself. Because the question of whether something constitutes fair use is a "legal judgment," proper consideration of the doctrine must include at least some analysis of the legal import of the facts. The Court concludes that at minimum, for the reasons discussed at length in its prior order, *see Lenz*, 572 F.R. Supp. 2d at 1154-56, a copyright owner must make at least an initial assessment as to whether the fair use doctrine applies to the use in question in order to make a good faith representation that the use is not "authorized by law."³⁸³⁹

However, in an interesting further analysis, the court rejected Lenz's argument that Universal's admitted failure to consider fair use before sending its takedown notices was by itself sufficient to impose liability under Section 512(f). The court noted the Ninth Circuit had held in *Rossi v. Motion Picture Assoc. of America, Inc.*³⁸⁴⁰ that the "good faith belief" requirement in Section 512(c)(3)(A)(v) encompasses a subjective, rather than objective, standard, and an unknowing mistake, even if the copyright owner acted unreasonably in making the mistake, is not sufficient for liability. In view of *Rossi*, the court concluded that Universal's mere failure to consider fair use would be insufficient to give rise to liability under Section 512(f). Instead, Lenz must demonstrate that Universal had some actual knowledge that its takedown notice contained a material misrepresentation.³⁸⁴¹

In the court's earlier opinion, it had ruled that Section 512(f) liability could attach upon a showing that the copyright owner acted in bad faith by issuing a takedown notice without proper consideration of the fair use doctrine. Although a bad faith requirement would be consistent

³⁸³⁸ *Id.* at *14-15.

³⁸³⁹ *Id.* at *17-18 (citation omitted).

³⁸⁴⁰ 391 F.3d 1000 (9th Cir. 2004).

³⁸⁴¹ *Lenz*, 2013 U.S. Dist. LEXIS 9799 at *18-19.

with Rossi's subjective standard, the court noted that neither the DMCA nor the applicable case law uses the term "bad faith." Instead, both frame the inquiry in terms of whether the party that issued the takedown notice had a "good faith belief" that use of the copyrighted work was unauthorized. Lenz asserted Universal's procedures for evaluating copyright infringement were so deficient that Universal willfully blinded itself as to whether any given video might constitute fair use. The court, citing authority that willful blindness is tantamount to knowledge, ruled that willful blindness could be sufficient to show an absence of good faith under Rossi's subjective standard. In the instant case, because the record was devoid of evidence that Universal subjectively believed that fair use might apply to Lenz's video, the court concluded that the only other avenue available to Lenz was to show that Universal willfully blinded itself to the potential application of the fair use doctrine.³⁸⁴²

To establish willful blindness, a plaintiff must establish that (1) the defendant subjectively believed there was a high probability that a fact existed and (2) the defendant took deliberate actions to avoid learning of that fact. The court noted that a trier of fact could conclude the second prong of this test was satisfied from the fact that Universal assigned the task of reviewing YouTube postings for infringing uses of Prince's songs to a single person who was not given any information or training about fair use. However, with respect to the first prong, Lenz had not submitted evidence suggesting that Universal subjectively believed either that there was a high probability that any given video might make fair use of a Prince composition or that her video in particular made fair use of Prince's song "Let's Go Crazy." Accordingly, the court concluded that Lenz was not entitled to summary judgment based on the theory that Universal willfully blinded itself to the possibility that her video constituted fair use. Nor was Universal entitled to summary judgment, as it had not shown that it *lacked* a subject belief that there was a high probability that any given video might make fair use of a Prince composition.³⁸⁴³

Finally, the court turned to Universal's contention that even if its takedown notice did contain a material misrepresentation sufficient to give rise to Section 512(f) liability, it was nonetheless entitled to summary judgment because Lenz could not demonstrate that she suffered any damages. The court rejected Universal's argument, affirming its previous ruling that had granted Lenz partial summary judgment with respect to Universal's third affirmative defense asserting that Lenz had not suffered any damages. Lenz asserted three categories of damages: loss of YouTube's hosting services and chilling of her free speech, lost time and resources, and attorneys' fees and costs. The court concluded that Lenz could not demonstrate damages based upon the loss of YouTube's hosting services and the chilling of her free speech. With respect to lost time and resources, Lenz requested that she be compensated at minimum wage for at least ten hours she spent before filing her lawsuit on obtaining counsel, figuring out how to send counternotices to YouTube and ensuring that her video was restored to YouTube. The court noted there was no reported case indicating definitively whether Lenz could recover

³⁸⁴² Id. at *19-21 & n.3.

³⁸⁴³ Id. at *21-23. The court rejected Lenz's argument that fair use was "self-evident" in the video, because a legal conclusion that fair use was self-evident necessarily would rest upon an objective measure rather than the subjective standard required by Rossi. Id. at *22-23.

for the time and resources she had expended, but she might be able at least to recover minimal expenses for electricity to power her computer, Internet and telephone bills and the like. With respect to attorneys' fees and costs, the court noted that, although an attorney at the Electronic Frontier Foundation (EFF) had helped Lenz prior to commencement of litigation on a *pro bono* basis, it was not clear that the attorney's equivalent normal billing rate for the time spent on this pre-litigation work could not form the basis for a damages claim. Lenz had pointed to language in her retainer agreement with EFF requiring her to assign any recovery up to the full amount of EFF's fees and expenses. The court therefore concluded that Lenz might recover the *pro bono* fees if she prevailed on her DMCA claim. Accordingly, the court denied Universal's motion for summary judgment that Lenz was precluded from recovering any damages for her DMCA claim. The court certified its summary judgment order for interlocutory appeal and stayed proceedings in district court pending resolution of the appeal.³⁸⁴⁴

The Ninth Circuit's Decision

On appeal, the Ninth Circuit affirmed the district court's order denying the parties' cross-motions for summary judgment, ruling that the DMCA requires copyright holders to consider fair use before sending a takedown notification, and that there was a triable issue in this case as to whether Universal formed a subjective good faith belief that the use was not authorized by law.³⁸⁴⁵

³⁸⁴⁴ *Id.* at *24-29. In its previous opinion, the court had ruled that fees incurred during litigation were not recoverable. Universal argued that EFF's pre-litigation work was so intertwined with the litigation that the pre-litigation fees should not be recoverable. Universal had not cited authority holding that "intertwined" fees are not recoverable, and the court was not prepared to conclude on the record before it that in fact the pre-litigation and post-litigation fees were so intertwined that the former would not be recoverable under the court's prior ruling. *Id.* at *29 n. 6.

³⁸⁴⁵ *Lenz v Universal Music Corp.*, 815 F.3d 1145, 1148 & 1158 (9th Cir. 2016). This opinion was an amended version of an earlier opinion the Ninth Circuit had issued on Sept. 17, 2015 at 801 F.3d 1145. The Ninth Circuit ordered the earlier opinion to be amended by order dated Mar. 17, 2016, which order also denied Universal's petition for panel rehearing. *Lenz v. Universal Music Corp.*, 2016 U.S. App. LEXIS 5025 (9th Cir. Mar. 17, 2016). The principle difference between the amended opinion and the earlier opinion is that the Ninth Circuit *deleted* the following paragraphs from the majority opinion that were previously found at 801 F.3d at 1135-36:

In order to comply with the strictures of § 512(c)(3)(A)(v), a copyright holder's consideration of fair use need not be searching or intensive. We follow *Rossi's* guidance that formation of a subjective good faith belief does not require investigation of the allegedly infringing content. *See 391 F.3d at 1003, 1005.* We are mindful of the pressing crush of voluminous infringing content that copyright holders face in a digital age. But that does not excuse a failure to comply with the procedures outlined by Congress. *Cf. Lenz, 572 F. Supp. 2d at 1155* ("[I]n the majority of cases, a consideration of fair use prior to issuing a takedown notice will not be so complicated as to jeopardize a copyright owner's ability to respond rapidly to potential infringements. The DMCA already requires copyright owners to make an initial review of the potentially infringing material prior to sending a takedown notice; indeed, it would be impossible to meet any of the requirements of *Section 512(c)* without doing so. A consideration of the applicability of the fair use doctrine simply is part of that initial review.").

To determine whether Section 512(c)(3)(A)(v) requires copyright holders to consider whether potentially infringing material is a fair use, the Ninth Circuit first resolved a dispute between the parties whether fair use is an authorization under the law as contemplated by Section 512(c), an issue which the Ninth Circuit noted was one of first impression in any circuit court. The Ninth Circuit agreed with the district court that Section 512(c) unambiguously contemplates fair use as a use “authorized ... by the law.” The Ninth Circuit ruled that fair use is not just excused by the law – i.e., it is not just a defense to infringement – but rather is wholly authorized by the law by virtue of the fact that Section 107 provides that “the fair use of a copyrighted work ... is not an infringement of copyright.”³⁸⁴⁶ The court then went on to hold that even if, as Universal argued, fair use is classified as an affirmative defense, for purposes of the DMCA fair use is uniquely situated in copyright law so as to be treated differently from traditional affirmative defenses. The court concluded that, because Section 107 created a type of non-infringing use, fair use is “authorized by the law” and a copyright holder must consider the existence of fair use before sending a takedown notice under Section 512(c).³⁸⁴⁷

To comply with its obligation to consider fair use before sending a takedown notice under Section 512(c), a copyright holder must form a subjective good faith belief that a use is not authorized by fair use. The Ninth Circuit noted that the relevant inquiry here was not whether a court would adjudge the video as a fair use (an objective standard), but whether Universal formed a good faith belief that it was not (a subjective standard). A copyright owner cannot be

We note, without passing judgment, that the implementation of computer algorithms appears to be a valid and good faith middle ground for processing a plethora of content while still meeting the DMCA's requirements to somehow consider fair use. *Cf. Hotfile*, 2013 U.S. Dist. LEXIS 172339, 2013 WL 6336286, at *47 (“The Court . . . is unaware of any decision to date that actually addressed the need for human review, and the statute does not specify how belief of infringement may be formed or what knowledge may be chargeable to the notifying entity.”). For example, consideration of fair use may be sufficient if copyright holders utilize computer programs that automatically identify for takedown notifications content where: “(1) the video track matches the video track of a copyrighted work submitted by a content owner; (2) the audio track matches the audio track of that same copyrighted work; and (3) nearly the entirety . . . is comprised of a single copyrighted work.” Brief for The Org. for Transformative Works, [**23] Public Knowledge & Int'l Documentary Ass'n as Amici Curiae Supporting Appellee at 29-30 n.8 (citing the Electronic Frontier Foundation website (link unavailable)).

Copyright holders could then employ individuals like Johnson to review the minimal remaining content a computer program does not cull. *See* Brief for The Recording Indus. Ass'n of Am. as Amici Curiae Supporting Appellants at 15 (“[T]he RIAA has an entire department dedicated to identifying infringement and issuing takedown requests.”); *see also Hotfile*, 2013 U.S. Dist. LEXIS 172339, 2013 WL 6336286, at *14. During oral argument Universal explained that service providers now use screening algorithms. However, we need not definitively decide the issue here because Universal did not proffer any evidence that – at the time it sent the takedown notification to Lenz – it used a computer program to identify potentially infringing content.

³⁸⁴⁶ *Lenz*, 815 F.3d at 1151-52. The court noted that fair use may sometimes be labeled as an affirmative defense due to the procedural posture of a particular case, as the Supreme Court apparently did in *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 573 (1994) (stating that “fair use is an affirmative defense” where the district court converted a motion to dismiss based on fair use into a motion for summary judgment).

³⁸⁴⁷ *Lenz*, 815 F.3d at 1153.

liable simply because an unknowing mistake was made, even if the copyright owner acted unreasonably in making the mistake.³⁸⁴⁸

Thus, Universal could face liability under Section 512(f) if it knowingly misrepresented in the takedown notice that it had formed a good faith belief the video was not authorized by the law – i.e., did not constitute fair use. Here, Lenz presented evidence that Universal did not form any subjective belief about the video’s fair use one way or another because it failed to consider fair use at all, and knew that it failed to do so. Universal contended that its procedures, while not formally labeled consideration of fair use, were tantamount to such consideration. The court ruled that a jury must therefore determine whether Universal’s actions were sufficient to form a subjective good faith belief about the video’s fair use or lack thereof.³⁸⁴⁹ The court summed up the legal rules as follows:

To be clear, if a copyright holder ignores or neglects our unequivocal holding that it must consider fair use before sending a takedown notification, it is liable for damages under § 512(f). If, however, a copyright holder forms a subjective *good faith* belief the allegedly infringing material does not constitute fair use, we are in no position to dispute the copyright holder’s belief even if we would have reached the opposite conclusion. A copyright holder who pays lip service to the consideration of fair use by claiming it formed a good faith belief when there is evidence to the contrary is still subject to § 512(f) liability.³⁸⁵⁰

The Ninth Circuit then turned to whether the willful blindness doctrine may be used to determine whether a copyright holder knowingly materially misrepresented that it held a good faith belief the offending activity was not a fair use, and concluded that it may. But, based on the specific facts presented during summary judgment in this case, the court rejected the district court’s conclusion that Lenz could proceed to trial under a willful blindness theory. The Ninth Circuit noted that to demonstrate willful blindness, a plaintiff must establish two factors: (1) the defendant subjectively believed that there was a high probability that a fact existed and (2) the defendant took deliberate actions to avoid learning of that fact. Lenz had failed to provide any evidence from which a juror could infer that Universal was aware of a high probability the video constituted fair use. The district court had denied Universal’s motion for summary judgment on the willful blindness theory because Universal had not shown that it *lacked* a subjective belief. The Ninth Circuit ruled this improperly required Universal to meet its burden of persuasion, even though Lenz had failed to counter the initial burden of production that Universal successfully

³⁸⁴⁸ *Id.* at 1153-54.

³⁸⁴⁹ *Id.* at 1154. The dissent argued that no triable issue fact existed because Universal did not specifically and expressly consider the fair use elements of Section 107. The majority rejected this position, noting that the question is whether the analysis Universal did conduct of the video was sufficient, not to conclusively establish as a matter of law that the video’s use of “Let’s Go Crazy” was fair, but to form a subjective good faith belief that the video was infringing on Prince’s copyright. And under the circumstances of this case, that question was for the jury, not the court, to decide. *Id.* at 1154 n.3.

³⁸⁵⁰ *Id.* at 1154.

carried. Accordingly, the Ninth Circuit ruled that Lenz could not proceed to trial on a willful blindness theory.³⁸⁵¹

Finally, the Ninth Circuit turned to the types of damages that Lenz might be able to recover, holding that a plaintiff may seek recovery of nominal damages for an injury incurred as a result of Section 512(f) misrepresentation and need not prove actual monetary loss. The court ruled, however, that Lenz could not recover nominal damages for impairment of her free speech rights. She could, however, potentially recover her expenses following the initiation of the Section 512(f) suit or costs and the reasonable value of the time incurred by her *pro bono* attorneys.³⁸⁵²

(vii) UMG Recordings v. Augusto

In UMG Recordings, Inc. v. Augusto,³⁸⁵³ UMG brought a claim for copyright infringement based on Augusto's sale on eBay of copies of promotional CDs he had received from UMG in advance of general commercial release. The promotional CDs had been labeled with language stating that they were licensed to the intended recipient for personal use only and that acceptance of the CD constituted an agreement to comply with the terms of the license, which prohibited resale or transfer of possession. UMG sent notices to eBay under the DMCA alleging that sale of the promotional CDs was infringing, in response to which eBay temporarily stopped Augusto's auctions and suspended his eBay account, although eventually his account was restored.³⁸⁵⁴ The court rejected UMG's claim for copyright infringement, ruling that the distributions of the CDs should be treated as "sales" for purpose of the first sale doctrine, notwithstanding the "license" agreement because recipients were free to keep the copies forever, UMG received no recurring benefit from recipients' continued possession, and the transfer was properly characterized as a gift, both under common law and under the Postal Reorganization Act.³⁸⁵⁵

Augusto brought a counterclaim against UMG under Section 512(f), alleging that UMG knowingly misrepresented to eBay that Augusto's auction infringed UMG's copyrights. The court rejected this claim because the evidence demonstrated that UMG had a subjective good faith belief that Augusto was infringing its copyrights. UMG was aware that Augusto had entered into a consent judgment in a previous case, in which he had admitted that selling promotional CDs violated the owner's copyright. Augusto also believed that the license language on the CDs

³⁸⁵¹ Id. at 1155-56.

³⁸⁵² Id. at 1156-57 & n.5.

³⁸⁵³ 558 F. Supp. 2d 1055 (C.D. Cal. 2008), aff'd, 628 F.3d 1175 (9th Cir. 2011).

³⁸⁵⁴ Id. at 1058.

³⁸⁵⁵ Id. at 1060-61. The Ninth Circuit affirmed this ruling with respect to the first sale doctrine. See UMG Recordings, Inc. v. Augusto, 628 F.3d 1175 (9th Cir. 2011).

enabled it to enforce its copyrights against an unauthorized seller of those CDs. Accordingly, the court granted UMG summary judgment on Augusto's Section 512(f) claim.³⁸⁵⁶

(viii) Capitol Records v. MP3tunes

In Capital Records, Inc. v. MP3tunes, LLC,³⁸⁵⁷ a number of record labels brought claims for copyright infringement against MP3tunes.com for offering online storage lockers where users could store illegally downloaded music and against sideload.com, a search engine that allowed users to search for free music downloads. The plaintiffs sent MP3tunes a DMCA take-down notice with a representative list of over 350 songs that were copied, performed, stored, distributed, and made available for download on or by MP3tunes, but also demanded that MP3tunes take action with respect to all of the plaintiffs' copyrighted recordings, even if not included on the representative list. MP3tunes removed the songs identified on the representative list from its websites, but took no action concerning the broader demand to take down other copyrighted recordings.³⁸⁵⁸

MP3tunes brought a counterclaim under Section 512(f) based on the allegation that five or more recordings on the take-down notice were authorized by one of the plaintiff record labels (EMI) for free downloading. The court ruled that MP3tunes was collaterally estopped from bringing the counterclaim based on an earlier ruling in a separate state litigation between the parties. MP3tunes then sought to amend its counterclaim to enumerate additional allegations, including that plaintiff EMI paid third parties to distribute free MP3s over the Internet; at least six of the plaintiffs' record label websites distributed songs for free; and EMI engaged in active marketing of its music directly and through hundreds or thousands of online music partners. The court denied MP3tunes the ability to amend its counterclaim on three grounds. First, the court noted, citing the Diebold case above, that a material misrepresentation for purposes of Section 512(f) is one that affected the infringer or service provider's response to a DMCA letter. Because MP3tunes removed only the songs on the representative list and did not respond to the demand that it remove all links to any of the plaintiffs' copyrighted recordings, the court concluded that the plaintiffs' representation that any link to its copyrighted recording was infringing could not be a "material" misrepresentation. Second, the court noted that MP3tunes had suffered no injury because it took no action other than filing an anticipatory lawsuit. Third, the court held that an allegation of a possibility that some of the songs on the representative list might be non-infringing was too speculative to meet applicable pleading standards, so amendment of the counterclaim would be futile.³⁸⁵⁹

³⁸⁵⁶ 559 F. Supp. 2d at 1065. The Ninth Circuit did not reach the issue under Section 512(f).

³⁸⁵⁷ 611 F. Supp. 2d 342 (S.D.N.Y. 2009).

³⁸⁵⁸ Id. at 344.

³⁸⁵⁹ Id. at 346-47.

(ix) Brave New Films v. Weiner

In Brave New Films 501(C)(4) v. Weiner,³⁸⁶⁰ Brave New Films uploaded to YouTube a video containing footage from The Michael Savage Show in which Savage made disparaging remarks about Muslims. The uploaded video criticized Savage's remarks. The syndicator of Savage's show, Original Talk Radio Network (OTRN), sent a DMCA takedown notice to YouTube, alleging that the video posted by Brave New Films was infringing. Brave New Films submitted a counter-notice to YouTube and instituted a lawsuit against Savage and OTRN, seeking a declaratory judgment that the video did not infringe copyrights held by OTRN or Savage, and alleging misrepresentation in violation of Section 512(f).³⁸⁶¹

Savage sought to avoid the Section 512(f) claim against him by arguing that the takedown notice submitted to YouTube by OTRN was defective, in that it did not allege a good faith belief that Brave New Films' use of the video was unauthorized, and that a notice not in compliance with all requirements of Section 512(c)(3)(A) could not form the basis for a Section 512(f) claim. The court rejected Savage's arguments on two grounds. First, OTRN stated in its takedown notice under penalty of perjury that the information in the letter was accurate and that YouTube had posted the video without authorization, which the court held was sufficient to satisfy the "good faith belief" requirement of Section 512(c)(3)(A). Second, the court ruled that the safe harbor provision of Section 512(c)(3)(A) and its attendant requirements are to protect OSPs from liability and cannot be asserted as a defense to Section 512(f) claims.³⁸⁶²

(x) Cabell v. Zimmerman

In Cabell v. Zimmerman,³⁸⁶³ the plaintiff alleged that the defendant, on behalf of the Actors' Equity Association (AEA), improperly caused his proprietary material to be blocked from YouTube. AEA had rights to control public display of works created pursuant to the terms of a contract between AEA and its member actors, presumably to ensure that its actors received royalties from any public display of their work. AEA sent a takedown notice to YouTube alleging that the plaintiff's video, "Pretty Faces," was infringing because it was subject to an AEA contract. The plaintiff responded to YouTube and AEA with an email expressing anger that access to Pretty Faces and certain other videos had been disabled without prior notification to him. An AEA representative responded to the plaintiff, explaining that when he sent the takedown notice to YouTube, he believed that Pretty Faces was subject to an AEA contract. He also explained that he had since done some research and discovered that Pretty Faces was not, in fact, subject to an AEA contract and apologized for the confusion. By the time of this lawsuit,

³⁸⁶⁰ 626 F. Supp. 2d 1013 (N.D. Cal. 2009). For an analysis of subsequent proceedings in this case, see Section III.C.6(b)(1)(iii).t above.

³⁸⁶¹ *Id.* at 1014-15.

³⁸⁶² *Id.* at 1017-18.

³⁸⁶³ 2010 U.S. Dist. LEXIS 25486 (S.D.N.Y. Mar. 12, 2010).

it was uncontested that the plaintiff owned the Pretty Faces copyright and that the takedown notice was sent to YouTube in error.³⁸⁶⁴

The plaintiff filed a claim for copyright infringement, arguing that the defendant had violated his exclusive rights to distribute and publicly display his video. Although the plaintiff acknowledged that the defendant never copied his work, the plaintiff asserted that the defendant interfered with the plaintiff's rights to distribute and publicly display his work on YouTube by preventing him from publicly displaying it. The court rejected this theory of copyright liability, but suggested that a claim like the plaintiff's claim could be appropriately raised under Section 512(f) (although the plaintiff had not done so). The court noted, however, that as a prerequisite to liability under section 512(f), a defendant must have actual knowledge that it is making a misrepresentation of fact. The plaintiff's complaint had alleged no facts from which a court could find it facially plausible that the defendant knew he was misrepresenting the facts when he wrote to YouTube and stated that the Pretty Faces video was infringing. The court noted that in pleading a claim for libel (not the copyright claim), the plaintiff stated that the defendant did not perform the proper due diligence to back up its claim that the plaintiff was a copyright infringer before sending a takedown notice to YouTube. The court noted, however, that negligence is not the standard for liability under Section 512(f). The court further noted that in an email sent by a representative of AEA two days after AEA sent its takedown notice to YouTube, the representative stated that the clips from Pretty Face had been submitted to him by someone claiming that the video had been filmed with AEA actors, he had taken in blind faith that the person was correct but had now determined that this was in error, and apologized. The court found that because this email, on which the plaintiff relied, stated on its face that the author did not act with actual knowledge when he sent the takedown notice to YouTube, there could be no liability under Section 512(f). Accordingly, the court granted the defendant's motion to dismiss.³⁸⁶⁵

(xi) Design Furnishings v. Zen Path

In Design Furnishings, Inc. v. Zen Path LLC,³⁸⁶⁶ the court ruled that notices to eBay that sales of wicker furniture on the eBay website infringed the Zen Path's copyrights violated Section 512(f). Zen Path's copyright registrations indicated a strong inference that it knew subjectively it did not have a valid copyright infringement claim when it filed its notices of infringement with eBay for two reasons. First, Zen Path's applications for copyright registration claimed its works were sculptures or three dimensional artwork or ornamental designs. However, the pictures of the furniture submitted by Zen Path with the copyright registrations suggested that Zen Path

³⁸⁶⁴ Id. at *1-2.

³⁸⁶⁵ Id. at *7-13.

³⁸⁶⁶ 2010 U.S. Dist. LEXIS 112314 (E.D. Cal. Oct. 21, 2010).

sought protection of the industrial design of the furniture. Second, the applications contained internal contradictions that the court did not elaborate.³⁸⁶⁷

(xii) Amaretto Ranch Breedables v. Ozimals

In Amaretto Ranch Breedables v. Ozimals, Inc.³⁸⁶⁸ the court denied a TRO and preliminary injunction barring Linden Research, operator of Second Life, from removing the plaintiff's virtual animal products from its site as a result of takedown notices issued by the defendant. The plaintiff alleged that the notices violated Section 512(f). The court found that the plaintiff had shown insufficient likelihood of success on the merits to support its Section 512(f) claim because the only similarity between the plaintiff's and the defendant's virtual animals was the idea that they each required "food" to "live."³⁸⁶⁹

(xiii) Shropshire v. Canning

In Shropshire v. Canning,³⁸⁷⁰ the plaintiff, owner of the musical composition "Grandma Got Run Over By A Reindeer," issued a takedown notice to YouTube to remove a video posted by the defendant containing pictures of reindeer with audio of a group called the "Irish Rovers" singing the plaintiff's composition. YouTube removed the video, the defendant then filed a counter-notice, stating that he believed the video constituted fair use of the composition, and YouTube restored the video. The plaintiff asserted a claim that the counter-notice was false under Section 512(f) and the defendant made a motion to dismiss.³⁸⁷¹

The court granted the motion. The court noted in passing that under Lenz v. Universal Music Corp.,³⁸⁷² a complainant filing a takedown notice must evaluate whether the material made fair use of the copyright. But in this instance, the Section 512(f) claim was being brought by the original complainant against the filer of a counter-notice. In any event, the court found the plaintiff had failed to identify a specific misrepresentation in the defendant's counter-notice. Accordingly, the court granted the motion to dismiss with leave to amend the plaintiff's complaint to identify a specific misrepresentation in the counter-notice and explain how that misrepresentation caused the plaintiff injury.³⁸⁷³

The plaintiff filed an amended complaint and the defendant again moved to dismiss. This time, the court granted the defendant's motion in part and denied it in part. The court denied the motion in part because the plaintiff had pled sufficient facts to show that the defendant did

³⁸⁶⁷ Id. at 8-10.

³⁸⁶⁸ 2010 U.S. Dist. LEXIS 141242 (N.D. Cal. Dec. 21, 2010).

³⁸⁶⁹ Id. at *2-7.

³⁸⁷⁰ 2011 U.S. Dist. LEXIS 4025 (N.D. Cal. Jan. 11, 2011).

³⁸⁷¹ Id. at *1-4.

³⁸⁷² 572 F. Supp. 2d 1150, 1154 (N.D. Cal. 2008).

³⁸⁷³ Shropshire, 2011 U.S. Dist. LEXIS 4025 at *17-18.

not have a good faith belief that the video was removed due to mistake or misidentification, as asserted in the counter-notice. The plaintiff had pled that that communications between its representative and the defendant prior to the counter-notice established that the defendant knew the material had not been removed due to a mistake or misidentification. Specifically, the amended complaint alleged that the plaintiff's representative had contacted the defendant several times to inform him that the "Grandma" song video infringed the plaintiff's copyright and that the defendant needed to obtain a license before issuing a counter-notice. The representative had also explained to the defendant the difference between rights to a copyrighted sound recording and a copyrighted composition, thereby clarifying to the defendant how the plaintiff could have a copyright interest in a recording performed by the Irish Rovers. Finally, the defendant had sent an email to the plaintiff stating "[g]o ahead, contact the Video site managers and get my video removed."³⁸⁷⁴

The court, however, granted the defendant's motion to dismiss insofar as it was based on a statement in the counter-notice that "[n]o sound was copied, no visuals were copied." The court found it was clear in context that this statement was referring to the fact that the audio in the defendant's video had been performed by the Irish Rovers and not copied from any video of performance of the Grandma song by the plaintiff. The court also interpreted a related statement in the counter-notice – that "no part of [the] Grandma video is a copy of any original work made by Elmo" – in a similar fashion. Accordingly, the court granted the defendant's motion to dismiss to the extent the Section 512(f) claim was based on these statements.³⁸⁷⁵

(xiv) Rock River Communications v. Universal Music Group

The case of Rock River Communications, Inc. v. Universal Music Group, Inc.³⁸⁷⁶ presented an interesting interpretation of the types of takedown demands to which Section 512(f) applies. The plaintiff created in 2006 certain remixed recordings of reggae music originally recorded by Bob Marley and the Wailers between 1969 and 1972. Universal Music Group controlled the rights to a large percentage of Marley's recordings and claimed it had acquired an exclusive interest in the recordings. Universal sent a cease and desist letter to Apple with respect to the sale of the plaintiff's album in Apple's iTunes online store. The plaintiff contended that Universal's letter contained knowing misrepresentations that the album was infringing, and that it was a takedown notice pursuant to Section 512(c)(3) and therefore subject to the prohibitions of Section 512(f).³⁸⁷⁷

The court granted summary judgment to Universal on the Section 512(f) claim on the ground that the cease and desist letter was not a DMCA takedown notice issued pursuant to Section 512(c) because it was not directed against materials posted at the direction of users.

³⁸⁷⁴ Shropshire v. Canning, 809 F. Supp. 2d 1139, 1141, 1148 (N.D. Cal. 2011).

³⁸⁷⁵ Id. at 1149.

³⁸⁷⁶ 2011 U.S. Dist. LEXIS 46023 (C.D. Cal. Apr. 27, 2011).

³⁸⁷⁷ Id. at *2-3, *48-49.

Rather, the recordings had been posted on iTunes by Apple, not its users, as Apple chose all recordings that were available through iTunes. Accordingly, because the “notification” at issue was not a notification pursuant to the DMCA, no claim under Section 512(f) could stand.³⁸⁷⁸

Universal also argued that the DMCA was not applicable because Apple received a financial benefit directly attributable to the alleged infringement on the iTunes site and therefore could not qualify for the Section 512(c) safe harbor.³⁸⁷⁹ The court rejected this argument, with the following observation: “The Court’s conclusion should not be read to imply that an internet service provider’s inability to meet all of the safe harbor requirements takes a dispute entirely out of the ambit of the DMCA. Rather, the Court concludes only that where the manner of the alleged infringement is not of any of the types addressed in 17 U.S.C. §512(c), (d), or (e), notice of claimed infringement given is not a section 512(c)(3) notification and therefore not subject to section 512(f).”³⁸⁸⁰

(xv) Smith v. Summit Entertainment

In Smith v. Summit Entertainment LLC,³⁸⁸¹ the court denied the defendant’s motion to dismiss the plaintiff’s Section 512(f) claim because the plaintiff had adequately pled that the defendant had submitted a DMCA notice to a web site on which the plaintiff had posted a copy of his song falsely alleging that the song infringed the defendant’s copyright, when in fact the defendant’s complaint was that the song’s CD cover violated the defendant’s trademark in a series of films called the “Twilight Saga.” The plaintiff had stated on the song’s CD cover that it was “inspired by the twilight saga.” The plaintiff’s allegations in his complaint that the defendant had made an unquestionably false assertion in take down notices, and the song was taken down, was sufficient to plead a claim under Section 512(f).³⁸⁸²

(xvi) Ouellette v. Viacom

In Ouellette v. Viacom Int’l, Inc.,³⁸⁸³ the plaintiff brought claims under Section 512(f) against Viacom alleging that Viacom improperly issued takedown notices against various videos the plaintiff posted to YouTube containing Viacom programs together with the plaintiff’s critiques of those programs. The plaintiff claimed Viacom had failed to evaluate whether the plaintiff’s use of its material was fair use before issuing the takedown notices. A magistrate judge recommended that the claims be dismissed with prejudice because the plaintiff (who was pro se) did not plead facts sufficient to show that Viacom had actual knowledge the plaintiff made fair use in posting and critiquing the Viacom videos and that Viacom acted in subjective

³⁸⁷⁸ Id. at *49-50.

³⁸⁷⁹ Id. at *51 n.11.

³⁸⁸⁰ Id.

³⁸⁸¹ 2011 U.S. Dist. LEXIS 60246 (N.D. Ohio June 6, 2011).

³⁸⁸² Id. at *1-3, *7-8.

³⁸⁸³ 2012 U.S. Dist. LEXIS 33556 (D. Mont. Mar. 13, 2012).

bad faith in issuing its takedown notices. The magistrate judge also concluded that the plaintiff's allegation that Viacom used scanning software to identify infringing material without human review for fair use was insufficient to support a Section 512(f) claim because no facts were pled that Viacom had actual knowledge of the software's deficiencies.³⁸⁸⁴

Upon objection by the plaintiff to the magistrate judge's recommendations, the district court adopted the findings and recommendations of the magistrate judge in full.³⁸⁸⁵ In elaboration of the magistrate's recommendations, the district court noted that the Ninth Circuit had established a high bar for plaintiffs for Section 512(f) claims in the Rossi case,³⁸⁸⁶ under which a defendant can be liable only if it knew that the subject material was not infringing when it issued its takedown notices. Without such a standard, copyright owners like Viacom could face limitless lawsuits just by policing its material on the Internet. The district court ruled that, contrary to the plaintiff's argument that interrogatories were the correct means for him to discover Viacom's intent in issuing its takedown notices to YouTube, Section 512(f) required him to allege facts, at the pleading stage, that demonstrate Viacom acted without a good faith belief. The court agreed with the magistrate that the plaintiff had not pled any facts meeting the subjective standard or establishing that his videos were fair use of Viacom's copyrighted materials.³⁸⁸⁷

With respect to the plaintiff's allegation that Viacom's use of scanning software violated the good faith requirement, the district court noted that the essence of the plaintiff's objection was that Viacom's history established that it used its software to abuse the takedown process, a form of "Internet bullying." The court ruled that the plaintiff could not satisfy his burden under the DMCA by alleging that Viacom had acted improperly in the past with respect to others. Rather, the Rossi case required him to plead factual allegations that Viacom acted improperly in *his* case by pleading facts that Viacom knew that its scanning software was flagging his non-infringing videos and that Viacom issued takedown notices nonetheless. Because the plaintiff had not done so, he had failed to state a sufficient Section 512(f) claim. The court granted Viacom's motion for judgment on the pleadings.³⁸⁸⁸

On appeal, the Ninth Circuit affirmed in a brief two-paragraph decision ruling that the district court had properly dismissed the plaintiff's action because he had failed to allege facts sufficient to demonstrate some actual knowledge of misrepresentation on the part of the copyright owner, and the district court did not abuse its discretion by dismissing the plaintiff's second amended complaint without further leave to amend after concluding that the plaintiff

³⁸⁸⁴ Id. at *1, *11-13.

³⁸⁸⁵ Ouellette v. Viacom Int'l, Inc., 2012 U.S. Dist. LEXIS 68109 (D. Mont. Apr. 25, 2012), aff'd, 2016 U.S. App. LEXIS 23116 (9th Cir. Dec. 22, 2016).

³⁸⁸⁶ Rossi v. Motion Picture Ass'n of Am., Inc., 391 F.3d 1000 (9th Cir. 2004).

³⁸⁸⁷ Ouellette, 2012 U.S. Dist. LEXIS 68109 at *7-10.

³⁸⁸⁸ Id. at *10-11, *13.

received ample notice of the pleading requirements for his claim and had an opportunity amend his pleading.³⁸⁸⁹

(xvii) Tuteur v. Crosley-Corcoran

This case arose out of a polemic between two bloggers who hosted blogs taking diametrically opposed views on the safety and virtues of home birthing. After a particularly acrimonious exchange, the defendant posted a photograph of herself in which she made an obscene gesture with her middle finger to give the plaintiff “something else to go back to her blog and obsess about.”³⁸⁹⁰ The plaintiff, without the defendant’s permission, copied the photo and posted it on her blog. The defendant then sent a cease and desist letter to the plaintiff alleging copyright infringement and sent a DMCA takedown notice to the plaintiff’s web site provider. The plaintiff filed a claim under Section 512(f), alleging a material misrepresentation of infringing activity in the takedown notice.³⁸⁹¹

On a motion to dismiss, the court seriously questioned whether the plaintiff had stated a viable claim, giving the plaintiff twenty-one days to show cause why the complaint should not be dismissed. The court found that the takedown notice, which stated accurately that the defendant’s likeness had been copied without her express authorization and published by the plaintiff without permission, appeared to conform to the letter of the requirements of Section 512(c)(3). The court noted that it was true that if this were a lawsuit brought by the defendant against the plaintiff for copyright infringement, the plaintiff would have a plausible, and even dispositive, fair use affirmative defense.³⁸⁹² “But there is no requirement in the DMCA that a notice-giver inform the service provider of an infringer’s possible affirmative defenses, only that she affirm her good faith belief (as appears to be the case here) that the copyrighted material is being used without her (or her agent’s) permission. Seen in this light, there is no material misrepresentation by [the defendant] of infringement, as a viable cause of action under *section* 512(f)(1) would require.”³⁸⁹³ The court did not cite any of the cases requiring the notice provider to consider a fair use defense before submitting a takedown notice.

In a subsequent opinion after briefing by the parties and oral argument in response to the court’s order to show cause, the court again denied the defendant’s motion to dismiss.³⁸⁹⁴ The court noted that the key issue to be decided was the proper test of what is required of a copyright owner prior to filing a takedown notice, including the extent to which a defense of fair use must be considered. The court noted that the Ninth Circuit in Rossi had specifically rejected the imposition of an objective standard of review for gauging the reasonableness of a copyright

³⁸⁸⁹ Ouellette v. Viacom Int’l, Inc., 2016 U.S. App. LEXIS 23116 (9th Cir. Dec. 22, 2016).

³⁸⁹⁰ Tuteur v. Crosley-Corcoran, 2013 U.S. Dist. LEXIS 51606 at *2 (D. Mass. Apr. 10, 2013).

³⁸⁹¹ Id.

³⁸⁹² Id. at *7.

³⁸⁹³ Id. at *8.

³⁸⁹⁴ Tuteur v. Crosley-Corcoran, 961 F. Supp. 2d 333, 344 (D. Mass. 2013).

owner's conduct in notifying parties of an allegedly infringing web site, instead concluding that the "good faith belief" requirement under Section 512(c)(3)(A)(v) encompasses a subjective standard. And in enacting the DMCA, the court noted that Congress did not require that a notice giver verify that he or she had explored an alleged infringer's possible affirmative defenses prior to acting, only that he or she affirm a good faith belief that the copyrighted material was being used without permission. To have required more would have put the takedown procedure at odds with Congress's express intent of creating an expeditious, rapid response to potential infringement on the Internet.³⁸⁹⁵

Citing the Lenz case (discussed in Section III.C.6(b)(4)(vi) above), the plaintiff argued that a consideration of fair use was required to give meaning to Section 512(c)(1)(A)(v)'s requirement that the copyright owner's declaration state that the appropriation of the copyrighted material is not authorized by "the law." The court rejected this argument, noted that Lenz was only a district court decision, and in any event in a follow-up opinion the Lenz court had substantially retreated from its earlier ruling, acknowledging that in light of Rossi, the mere failure to consider fair use would be insufficient to give rise to liability under Section 512(f) and that a plaintiff must show that the defendant had some actual knowledge that its takedown notice contained a material misrepresentation.³⁸⁹⁶

In support of her motion to dismiss, the defendant stated that prior to sending the takedown notices she sought the advice of two attorneys. The second attorney submitted an affidavit stating that he considered, and rejected, the plaintiff's argument that her posting of the photo constituted fair use. The plaintiff objected to the court's consideration of this affidavit in deciding a motion to dismiss, arguing that any reliance on material outside the four corners of the complaint would impermissibly convert the motion to dismiss to one for summary judgment, notice of which the court had not provided to the parties under Rule 12(d). The court noted the complaint's allegations that the plaintiff's counsel had a Jan. 10, 2013 conversation with the defendant's second attorney in which he allegedly conceded that it was obvious the defendant had no copyright claim against the plaintiff. Because the attorney adamantly denied such assertion, the court found a dispute of material fact sufficient to defeat a brevis dismissal. Accordingly, the court concluded that a knowing and material misrepresentation had been adequately pled and denied the defendant's motion to dismiss.³⁸⁹⁷

(xviii) **Flava Works v. Gunter**

The facts of this case are discussed in Section III.C.2(m) above. myVidster asserted a counterclaim against Flava under Section 512(f). The court denied Flava's motion to dismiss the counterclaim, finding that it had been adequately pled. myVidster alleged that Flava knowingly misrepresented that certain infringing content was available on myVidster's web site despite having received notification from myVidster that the content had been removed, and that Flava

³⁸⁹⁵ Id. at 341-44.

³⁸⁹⁶ Id. at 343.

³⁸⁹⁷ Id. at 341& n.16, 344.

did so purposefully, in an effort to improperly exaggerate the actual amount of infringing content available on the myVidster.com web site. The court found that these allegations allowed one to draw a reasonable inference of liability and were sufficient to present a story that held together, which was all that was required under federal pleading standards.³⁸⁹⁸

(xix) Disney Enterprises v. Hotfile

The facts of this case are set forth in Section III.C.6(b)(1)(iii).y above. Hotfile brought a counterclaim against one of the plaintiffs, Warner Brothers, under Section 512(f) based on the fact that Warner had submitted several hundred erroneous takedown notices with respect to some content that it did not own, including a popular and innocuous free software program known as JDownloader, and had relied heavily on automated software technology to identify files for takedown without manual review of whether the files were actually infringing. Warner moved for summary judgment on the claim.³⁸⁹⁹

Both Warner and Hotfile agreed that Section 512(f) requires actual, subjective knowledge of the fact of noninfringement at the time that a takedown notice is made, but Hotfile argued that some of Warner's actions with respect to its takedown notices suggested that its mistaken takedown notices might rise to willful blindness or even actual knowledge. In particular, Hotfile argued that Warner's lack of pre-notice review, and its focus on determining whether it owned the works on the system, rather than whether the use of the works infringed its copyrights, supported liability under Section 512(f). The court noted that Warner's reliance on technology to accomplish the identification of files for takedown might have prevented it from forming any belief at all as to whether identified files were infringing. However, the court stated that it was unaware of any decision to date that actually addressed the need for human review, and the statute does not specify how belief of infringement may be formed or what knowledge may be chargeable to the notifying entity.³⁹⁰⁰

At bottom, the court concluded that, while there were engaging questions surrounding Warner's knowledge, its responsibility to investigate, whether it had a good faith belief in infringement in each instance, and whose burden it was to show or refute what (all issues of first impression in its Circuit), there was sufficient evidence in the record to suggest that Warner intentionally targeted files it knew it had no right to remove. Such evidence was sufficient to preclude summary judgment in Warner's favor. The only remaining issue with respect to the Section 512(f) claim was therefore whether Hotfile would be able to show any injury for the erroneous deletions, which is an element of a Section 512(f) claim. The court noted that the quantity of economic damages to Hotfile's system was necessarily difficult to measure with precision and there was much disagreement between the parties and their experts on the point. Notwithstanding such difficulty, the court found that the fact of injury had been shown by Hotfile, and its expert could provide the jury with a non-speculative basis to assess damages.

³⁸⁹⁸ Flava Works, Inc. v. Gunter, 2013 U.S. Dist. LEXIS 125294 at *6-7 (N.D. Ill. Sept. 3, 2013).

³⁸⁹⁹ Disney Enterprises, Inc. v. Hotfile Corp., 2013 U.S. Dist. LEXIS 172339 at *47-53 (S.D. Fla. Sept. 20, 2013).

³⁹⁰⁰ Id. at *149-56.

Accordingly, the court denied Warner's motion for summary judgment on the Section 512(f) claim.³⁹⁰¹

In Dec. 2013, the MPAA announced a settlement under which the district court had awarded damages of \$80 million to the plaintiffs and ordered Hotfile to either shut down its operations or use digital fingerprinting technology to prevent copyright infringement by its users.³⁹⁰²

(xx) Flynn v. Siren-Bookstrand

In this case, the plaintiff was the author of numerous books of fiction, with respect to which she had a series of contracts with the defendant to publish them. Each contract gave the defendant a right of first refusal to publish any book that was a sequel to the book covered in the contract. A dispute arose with respect to two of the author's books. The defendant requested that changes be made to the books, the author refused, and published the books herself on Amazon. The defendant claimed that the books were sequels to others of the author's books the defendant had published and sent takedown notices to Amazon, which took the books off its site in response. The plaintiff brought a claim against the defendant alleging that the takedown notices violated Section 512(f) because the defendant must have known, based on the parties' prior dealings, that it had no claim to the copyright in either book.³⁹⁰³

The plaintiff sought a temporary restraining order from the court, ordering the defendant to cooperate with her in instructing Amazon to restore access to the two books on its site and to enjoin the defendant from interfering further with her efforts to publish the books. The plaintiff argued that the defendant's violation of a federal statute – here, Section 512(f) of the DMCA – allowed the court to presume the existence of irreparable harm to her and the public for purposes of the injunctive relief she sought. The court noted it is true that, where Congress expressly provides for injunctive relief to prevent violations of a statute, a plaintiff need not demonstrate irreparable harm to secure an injunction. However, the plaintiff had not identified any portion of the DMCA providing for injunctive relief to remedy or prevent violations of Section 512(f), nor had the court identified any such provision. To the contrary, Section 512(f) provides solely for an award of damages. The plaintiff therefore was required to demonstrate irreparable harm under the traditional equitable factors for injunctive relief, which she had failed to do.³⁹⁰⁴

³⁹⁰¹ *Id.* at *156-58.

³⁹⁰² "Hotfile To Pay \$80M to MPAA, Studios In Copyright Suit," *Law360* (Dec. 3, 2013), available as of Dec. 7, 2013 at http://www.law360.com/ip/articles/493076?nl_pk=be5fde4e-8dc1-4d81-b621-f0352bcdff74&utm_source=newsletter&utm_medium=email&utm_campaign=ip.

³⁹⁰³ *Flynn v. Siren-Bookstrand, Inc.*, 2013 U.S. Dist. LEXIS 135095 at *1-5 (D. Neb. Sept. 20, 2013).

³⁹⁰⁴ *Id.* at *7-14.

(xxi) Crossfit v. Alvies (based on a trademark claim under the DMCA)

The case of CrossFit, Inc. v. Alvies³⁹⁰⁵ raised the interesting question of whether a takedown notice issued under the DMCA based on an alleged violation of a trademark, rather than a copyright, is proper. The plaintiff was the owner of a trademark in CROSSFIT pertaining to fitness training services. The defendant, a stay-at-home mother of four children, launched a blog at crossfitmamas.blogspot.com and created a “CrossFit Mamas” Facebook page. She used the blog to post daily high-intensity interval training routines. A CrossFit representative contacted the defendant and demanded that she stop using the CROSSFIT name on her blog and affiliated Facebook page. CrossFit also sent a DMCA takedown notice to Facebook. The defendant renamed her blog but a dispute continued over CrossFit’s demands that the defendant delete over two years of blog posts. CrossFit filed an action asserting trademark infringement, false designation of origin, trademark dilution and cyberpiracy. The defendant filed a counterclaim under Section 512(f), alleging that CrossFit made material misrepresentations in its DMCA takedown notice to Facebook. The defendant asserted that CrossFit’s invocation of the DMCA was improper and misleading because CrossFit’s claims were based on the assertion of trademark rights, not copyrights.³⁹⁰⁶

CrossFit moved to dismiss the counterclaim, arguing that the defendant’s claim was implausible because Facebook allowed trademark takedown notices as well as DMCA copyright takedown notices. The court rejected the argument. As an initial matter, the court found it unclear why it should take judicial notice of Facebook’s internal compliance procedures, which was not a fact generally known within the court’s discretion. But even if judicial notice were appropriate, the court found the defendant had plausibly alleged that CrossFit materially misrepresented that the defendant’s Facebook page infringed on a copyright, since CrossFit’s claims were based only on its asserted trademark rights. Whether CrossFit may have been able to convince Facebook to remove the defendant’s page on some other ground had no bearing on CrossFit’s compliance with the DMCA.³⁹⁰⁷

CrossFit also contended that the defendant’s counterclaim failed because she was not injured by the DMCA takedown notice. CrossFit argued that if it had not submitted a DMCA takedown notice, it could have submitted a trademark takedown notice that would have had the same effect. The court rejected this argument, finding that, essentially, CrossFit was asking the court to find that the defendant’s Facebook page infringed on CrossFit’s trademarks, and had CrossFit submitted a trademark takedown notice, Facebook would have removed the defendant’s page. The court noted that it could not adjudicate the merits of CrossFit’s trademark claims on a motion to dismiss the defendant’s counterclaim, let alone hypothesize about what Facebook would or would not have done if it had received a trademark takedown

³⁹⁰⁵ 2014 U.S. Dist. LEXIS 7930 (N.D. Cal. Jan. 22, 2014).

³⁹⁰⁶ Id. at *2-5, *6-7.

³⁹⁰⁷ Id. at *6-7.

notice regarding the defendant's Facebook page. Accordingly, the court denied CrossFit's motion to dismiss.³⁹⁰⁸

(xxii) Automattic v. Steiner

In Automattic v. Steiner,³⁹⁰⁹ the court adjudicated the extraterritorial effect of Section 512(f). The plaintiff Hotham was a student journalist residing in London who maintained a blog on WordPress.com, a web publishing platform operated by the other plaintiff in the case, Automattic. Hotham sent a list of questions to an organization called Straight Pride UK to find out more about the organization's goals. The defendant Steiner responded on behalf of Straight Pride UK, supplying answers to Hotham's questions in a document titled a "Press Statement." Hotham then published a blog on WordPress, commenting on Straight Pride UK and attaching the Press Statement. Steiner sent a DMCA takedown notice demanding that the blog be taken down, apparently because it reproduced the Press Statement. WordPress took the blog down. Following the removal of his blog post, Hotham posted more content to his blog on WordPress pertaining to the Press Statement.³⁹¹⁰ Steiner sent another takedown notice, asserting that Hotham was pursuing a course of conduct that amounted to harassment and was encouraging others to harass Straight Pride UK and repost his blog, which "contains our name, lines and wording to their blogs hosted on wordpress.com."³⁹¹¹ Automattic replied that it was in no position to arbitrate content disputes or make any form of legal judgment on allegations or claims, and requested that Steiner provide it with a formal court order including a court's decision regarding this particular content. Subsequently Steiner sent a third takedown notice directed at certain content posted by Hotham. Automattic and Hotham then brought claims against Steiner under Section 512(f).³⁹¹²

A magistrate judge recommended that Steiner be found in violation of Section 512(f) on the ground that he knowingly misrepresented that Hotham violated his copyright because Steiner could not have reasonably believed that the Press Statement he sent to Hotham was protected under copyright, and such misrepresentations were material because they induced Automattic to disable Hotham's article. The court further concluded that the fact that Steiner made his misrepresentations in London and not in the U.S. did not bar a claim under Section 512(f). The focus of Section 512(f) is not where the fraudulent misrepresentation originated, rather where the reliance, wrongful removal, and the resulting injury occurred. Here the allegedly infringing material was hosted by Automattic, a California corporation, and Steiner's takedown notices were directed to Automattic in California. Automattic's reliance on Steiner's

³⁹⁰⁸ Id. at *7-8.

³⁹⁰⁹ 82 F. Supp. 3d 1011 (N.D. Cal. 2014).

³⁹¹⁰ Id. at 1017-19.

³⁹¹¹ Id. at 1018.

³⁹¹² Id. at 1019.

misrepresentations and resulting injury also both occurred in California. Accordingly, Section 512(f) could be applied to Steiner's actions.³⁹¹³

With respect to damages, the magistrate recommended that Hotham be awarded \$360 for sixteen hours he spent researching the validity of the takedown notice, determining how to proceed and responding to media inquiries related to the incident, based on the value of his time and compensation when writing freelance articles, and \$600 in lost work based on the significant distraction from freelance work he would normally be doing. The court recommended that Automattic recover \$1,860 for the time three employees spent responding to Steiner's takedown notices and responding to related press inquiries, based on their salaries and a standard 2,000 hour year. The court also recommended that Automattic recover in full its request of \$22,264 in attorneys' fees for the hours reasonably expended on the litigation. Finally, the court recommended denial of Hotham's request for damages for reputational harm (which were too speculative), for his emotional distress (as there was no authority holding that emotional distress damages are available under Section 512(f)), and for chilling of his free speech (because Steiner was a private actor).³⁹¹⁴

The district court subsequently adopted the magistrate's recommendations in full, finding them to be correct, well-reasoned and thorough, and entered judgment accordingly against Steiner.³⁹¹⁵

(xxiii) *Distribuidora v. Guerra*

The plaintiffs had entered into two agreements with defendant Guerra under which they paid Guerra for certain rights to songs he promised to record. Plaintiffs uploaded recordings of several such songs onto Apple's iTunes store. Guerra contented he retained "administration rights" in the songs under the agreements, including the right to license the use of the songs and to collect publishing/songwriting royalties from licensees. Guerra's attorney submitted a takedown notice to Apple relating to the recordings, stating that Guerra was the publisher of the musical compositions embodied in the recordings and no license had been issued for the songs. Apple responded by removing the recordings from iTunes. The plaintiffs brought a claim against Guerra and his attorney under Section 512(f) for misrepresentation in the takedown notice and defendants moved to dismiss under Rule 12(b)(6).³⁹¹⁶

The defendants based their motion to dismiss on two grounds. First, the defendants argued that, because Section 512(f) requires that a person make the misrepresentation "under this section," the misrepresentation is actionable only when the notice containing the misrepresentation complies substantially with all the elements listed in Section 512(c)(3)(A). The

³⁹¹³ *Id.* at 1027-28.

³⁹¹⁴ *Id.* at 1029-32.

³⁹¹⁵ *Automattic Inc. v. Steiner*, 82 F. Supp. 3d 1011 (N.D. Cal. 2015).

³⁹¹⁶ *Distribuidora De Discos Karen, C por A. v. Guerra Seijas*, 2015 U.S. Dist. LEXIS 42636 at * 2-3, *8-9 (S.D.N.Y. Mar. 26, 2015).

court ruled that a takedown notice can be actionable under Section 512(f) even if it is, to some extent, technically deficient under Section 512(c)(3). Section 512(c)(3) is intended to protect the service provider, not to protect individuals who intentionally make false demands. Otherwise, a person could submit a slightly deficient takedown notice with impunity. The court concluded that the words “under this section” should not render Section 512(f) so toothless. The court acknowledged that a takedown notice could be so deficient that it is utterly unrecognizable as a takedown notice and therefore would not constitute a representation “under this section.” That would be the case if the notice failed to substantially comply with elements (ii) through (iv) of Section 512(c)(3)(A), because the notice would carry no legal effect. Here, however, the plaintiffs had adequately pled that the takedown notice substantially complied with elements (ii) through (iv), which was sufficient to make a Section 512(f) claim.³⁹¹⁷

Second, the defendants argued that a notice containing the misrepresentation is actionable under Section 512(f) only if directed toward infringement “by reason of the storage at the direction of a user.” The defendants argued that here, no music was stored on iTunes at the direction of a user (in particular, not at the plaintiffs’ direction), so the plaintiffs’ Section 512(f) claim must fail. Although the court agreed that the notice must be directed toward infringement by reason of the storage at the direction of a user, it noted that the key question here was whether Apple stores music on iTunes at the direction of a user. If so, then the attorney’s takedown notice was actionable under Section 512(f). The court ruled that it could not resolve the issue on a motion to dismiss. The court found that the Apple iTunes contract did not settle the question whether Guerra’s music was stored on iTunes at Apple’s or the plaintiffs’ direction. In particular, it was not clear who (if anyone) exercised discretion in selecting music for sale on iTunes once the Apple contract was signed. Although the contract required the plaintiffs to deliver to Apple every song they had the rights to deliver, it also assigned the plaintiffs the duty to determine whether they possessed the appropriate distribution rights.³⁹¹⁸

The court elaborated that the proper question was not whether Apple had the legal right to control how music appeared on iTunes (as it surely did), but rather the degree to which, as a practical matter, Apple actually exercised its rights by organizing the plaintiffs’ music on iTunes manually or deciding how to promote the plaintiffs’ music. The presence of some automated processing in between when the plaintiffs uploaded music and when the music appeared on iTunes for sale would not be enough to take iTunes outside the scope of Section 512(c). But if Apple routinely performed material, discretionary, manual functions on incoming songs, then iTunes might well fall outside the ambit of Section 512(c). In sum, the court concluded that the complaint simply did not state enough facts about iTunes for the court to determine what happened behind the scenes, so it could not decide at the present stage whether iTunes stores music at the direction of users. Accordingly, the court denied the motion to dismiss.³⁹¹⁹

³⁹¹⁷ Id. at *12-16.

³⁹¹⁸ Id. at *13, *17-20.

³⁹¹⁹ Id. at *20-23.

(xxiv) Handshoe v. Perret

In this case, the court ruled that the plaintiff, an individual, lacked statutory standing to pursue his claims under Section 512(f) because the takedown notices on which the claims were based were directed to published posts made by a third party, Slabbed New Media, LLC, not to those of the plaintiff individually. Nor was the plaintiff pursuing his own legal rights and interests in those claims, but rather the legal rights and interests of Slabbed New Media, LLC. Accordingly, the court dismissed the claims because the plaintiff lacked statutory standing to assert the claims on his own, individual behalf.³⁹²⁰

(xxv) ISE Entertainment v. Longarzo

In this case, ISE asserted that it was the owner of copyrights in a television series program. Amazon Video Direct notified ISE that it had suspended the program from Amazon Video's web site in response to a DMCA notice submitted by the defendant, who was an attorney for the co-producer of the program, claiming that the distribution of the program was unauthorized. Although a written agreement between ISE and the co-producer stated that copyrights in the program would belong to ISE, the co-producer asserted that ISE was in breach of the agreement and the posting of the program on the Amazon Video web site was therefore unauthorized. ISE brought a claim against the defendant under Section 512(f) alleging that the DMCA notice submitted by the defendant was false.³⁹²¹

The defendant argued that ISE did not have standing to bring a Section 512(f) claim because ISE never registered a copyright covering the program and was therefore not a "copyright owner." The court rejected this argument, pointing out that Section 512(f) provides that anyone who knowingly submits a false takedown notice to an OSP shall be liable for any damages, including costs and attorneys' fees, incurred by the "alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider." Thus, not only a copyright owner may assert Section 512(f), but also an alleged infringer, which ISE was, whether or not it had registered the copyright for which it asserted ownership. The court therefore held that neither copyright ownership nor registration are prerequisites to bringing a Section 512(f) action, and as an "alleged infringer," ISE had standing to sue under Section 512(f).³⁹²²

(xxvi) Stevens v. Vodka & Milk

In this case, the plaintiff owned the copyright in a song titled "Captain Save a Hoe." The plaintiff sent DMCA takedown notices to various online retailers asking that they stop selling the defendants' book, also titled "Captain Save a Hoe," which the plaintiff claimed infringed his copyright. The defendants brought a counterclaim of intentional interference with contract on the ground that the plaintiff knew or should have known that the takedown notices would cause

³⁹²⁰ Handshoe v. Perret, 270 F. Supp. 3d 915, 930 (S.D. Miss. 2017).

³⁹²¹ ISE Entm't Corp. v. Longarzo, 2018 U.S. Dist. LEXIS 40755 at *2-5 (C.D. Cal. Feb. 2, 2018).

³⁹²² Id. at *11-15.

the retailers to stop selling the book and thus breach their contracts with the defendants. The plaintiff argued that the defendants' counterclaim should be dismissed because it is preempted by the DMCA. The court agreed, ruling that the pervasive nature of the DMCA, including an express remedy for the very wrong that the defendants were alleging, made reasonable the inference that Congress left no room for the states to supplement the remedies outlined in the DMCA. Accordingly, the court dismissed the counterclaim with prejudice.³⁹²³

(xxvii) **Johnson v. New Destiny Christian Center Church**

The plaintiff operated a web site and YouTube channel on which she posted videos that included self-recorded portions of the defendant Paula White's sermons. The sermons were distributed online and on television by the entity Paula White Ministries (PWM). After PWM discovered the plaintiff's YouTube channel and videos containing PWM's intellectual property, PWM evaluated whether the videos constituted fair use. PWM's general manager decided that they were not fair use and so directed an employee to submit a series of takedown notices on behalf of PWM. Over the course of a couple of years, PWM sent numerous takedown notices to YouTube, the plaintiff responded with counter-notifications, PWM consulted an attorney to determine whether there was a reasonable basis for a copyright infringement claim against the plaintiff, and then filed a copyright lawsuit, which it later dismissed. An additional series of takedown notices and counter-notifications between the plaintiff and PWM ensued, until eventually the plaintiff filed this lawsuit against the defendants for, among other things, malicious prosecution and material misrepresentation under Section 512(f). The plaintiff alleged that the takedown notices were false from the start based on her contention that PWM and its attorneys did not have a subjective good faith belief when they contacted YouTube to remove her videos. The defendants moved for summary judgment on the Section 512(f) claim.³⁹²⁴

The district court noted that under the Ninth Circuit's Lenz decision (discussed in Section III.C.6(b)(4)(vi) above), a copyright holder must consider fair use before sending a takedown notice, and if the copyright holder forms a subjective good faith belief the allegedly infringing material does not constitute fair use, the court is in no position to dispute the copyright holder's belief even if it would have reached the opposite conclusion. But summary judgment should be denied if the copyright holder pays lip service to the consideration of fair use by claiming it formed a good faith belief when there is evidence to the contrary. The district court ruled that the evidence before it in this case uniformly supported the defendants' good faith defense and the plaintiff had not supplied a factual basis on which to find the opposite. The defendants submitted affidavits from its general manager and the attorney who brought the copyright infringement claim stating that before PWM sent YouTube takedown requests, the plaintiff's

³⁹²³ Stevens v. Vodka & Milk, LLC, 2018 U.S. Dist. LEXIS 43666 at *1-7 (S.D.N.Y. Mar. 15, 2018). See also Beyond Blond Prods. v. Heldman, 2020 U.S. Dist. LEXIS 150556 at *9 (C.D. Cal. Aug. 17, 2020) (DMCA preempts state law claims arising out of the submission of infringement notices); Stardock Sys., Inc. v. Reiche, 2019 U.S. Dist. LEXIS 229910 at * 11-12 (N.D. Cal. May 14, 2019) (same); Amaretto Ranch Breedables, LLC v. Ozimals, Inc., 2011 U.S. Dist. LEXIS 73853 at *3-5 (N.D. Cal. July 8, 2011) (an infringement notice is a "creature of a federal statutory regime" that preempts any state law claim based on the submission of such a notice).

³⁹²⁴ Johnson v. New Destiny Christian Ctr. Church, 2019 U.S. Dist. LEXIS 33513 at *1-9 (M.D. Fla. Mar. 4, 2019).

videos were analyzed to determine whether they constituted fair use. Each time, PWM concluded that the plaintiff's videos did not constitute fair use and were infringing copyrighted material. The plaintiff responded by offering her version of events, which the court found to be based exclusively on speculation. Although the plaintiff claimed certain inaccuracies in PWM's submissions to YouTube, she had not come forth with competent summary judgment evidence that called into question PWM's good faith belief. The court therefore granted the defendants summary judgment on the plaintiff's Section 512(f) claim.³⁹²⁵

(xxviii) Ningbo Mizhihe v. Does

The plaintiff was the owner of a registered copyright on a design for a unicorn. The defendants sold products containing a unicorn design, which the plaintiff believed infringed the copyright on its unicorn design. The plaintiff submitted multiple takedown notifications to Amazon, asserting that some of the defendants' unicorn-related products on the Amazon web site were infringing, in response to which Amazon removed several of the defendants' listings and disabled their online store. The defendant brought a counterclaim under Section 512(f), alleging in its counter-complaint that the plaintiff's unicorn designs were derivative of other unicorn designs widely available on ecommerce markets, and that if the Copyright Office had been made aware of the preexisting unicorn designs, it would have rejected the plaintiff's copyright registration applications.³⁹²⁶

The plaintiff filed a motion to dismiss the DMCA counterclaim on the basis that it had accurately represented to Amazon that it held certain copyrights and the defendants had not alleged facts to support a plausible inference that the plaintiff knowingly made a misrepresentation to Amazon. The court agreed on both points. With respect to the first point, the court noted that the defendants focused their arguments on a claim that the plaintiff made misrepresentations to the *U.S. Copyright Office*, not to Amazon, and that these alleged misrepresentations were fatal to the ultimate enforceability of the copyrights. The court found that the plaintiff had represented to Amazon that it owned several copyrights and the defendants' activity was infringing, which it believed in good faith to be the case, and made no representations whatsoever to Amazon regarding enforceability of its copyrights. The defendants would have the chance in due course to raise their argument as to unenforceability, but as a defense to liability rather than a counterclaim under Section 512(f).³⁹²⁷

With respect to the second point, the court ruled that even if it were enough for liability under Section 512(f) for the plaintiff to have notified Amazon of the existence of certain copyrights that were unlawfully secured, there was insufficient material in the pleadings to support an inference that the plaintiff *knew* its copyrights were not enforceable. And in any event the defendants' accusation that the plaintiff knowingly made misrepresentations was effectively an accusation of failing to perform an adequate investigation of the available prior art,

³⁹²⁵ *Id.* at *12-14.

³⁹²⁶ *Ningbo Mizhihe I&E Co. v. Does*, 2020 U.S. Dist. LEXIS 76724 at *1-3 (S.D.N.Y. Apr. 30, 2020).

³⁹²⁷ *Id.* at *6-7.

which sounded merely in negligence. Accordingly, the court dismissed the Section 512(f) counterclaim.³⁹²⁸

(xxix) Enttech Media Grp. V. Okularity

The plaintiff was the publisher of a magazine. The defendant Okularity used software that scanned the Internet for images that infringed on copyrighted photographs of its clients (also named as defendants in the lawsuit, who operated clearinghouse web sites for photographs), then automatically generated and filed DMCA take-down notices against purported infringers. Okularity waited until the notices accumulated to the point where a social media platform disabled the infringer's account before contacting the purported infringer to initiate settlement negotiations on behalf of its clients. The plaintiff brought a claim under Section 512(f), alleging that the defendants knowingly and materially misrepresented that copyright infringement occurred. The defendants filed a motion to dismiss the claim.³⁹²⁹

The plaintiff alleged that Okularity automatically generated DMCA notices without considering potential non-infringing use of images, including fair use. The court held that, read in the light most favorable to the plaintiff, such allegations constituted lack of a subjective good faith belief because if Okularity failed to consider fair use, it could not have formed a good faith belief that the images were infringing, and Okularity's bad faith belief is imputed to the other defendants through their agency relationship. Accordingly, the plaintiff had pled that the defendants made misrepresentations knowingly.³⁹³⁰

The court further held that the plaintiff sufficiently pled materiality because it alleged that Instagram disabled the plaintiff's account following the defendants' DMCA notices. The defendants argued that the misrepresentation could not have been material because the plaintiff never alleged that the images were non-infringing. The court rejected this argument because such allegation is irrelevant under Section 512(f), which imposes liability for lack of a good faith belief that the material was infringing at the time the complainant sent the take-down notice. Accordingly, the only relevant inquiry under Section 512(f) is whether the defendants formed a good faith belief that the images were infringing at the time they sent the take-down notices, the plaintiff had alleged that the defendants lacked good faith belief, and that was sufficient. The court therefore denied the defendants motion to dismiss the Section 512(f) claim.³⁹³¹

The plaintiff filed a third amended complaint and the defendant again moved to dismiss the Section 512(f) claim. The court noted that, to satisfy the "knowingly" prong of Section 512(f), the plaintiff must allege sufficient facts to show that the defendants lacked a subjective good faith belief that the images that were the subject of their takedown notices were infringing.

³⁹²⁸ Id. at *7-8.

³⁹²⁹ Enttech Media Grp. LLC v. Okularity, Inc., 2020 U.S. Dist. LEXIS 222489 at *1-2, *13 (C.D. Cal. Oct. 2, 2020).

³⁹³⁰ Id. at *13-14.

³⁹³¹ Id. at *14-15.

In arguing for dismissal, the defendants contended that by alleging that many or all of the plaintiff's DMCA takedown notices contained identical verbatim discussion of infringement and fair use, the plaintiff had effectively admitted that the defendants did in fact conduct infringement and fair use analysis before submitting their takedown notices.³⁹³²

The court noted that the plaintiff's allegation that the DMCA notices contained an analysis of infringement and fair use presented a question of first impression with respect to the standard for pleading a Section 512(f) claim. Specifically, was it sufficient for the plaintiff to allege that, notwithstanding the takedown notices' explicit and extensive fair use analysis, the defendants did not actually or sufficiently consider fair use before issuing a takedown notice? The court noted, at first blush, the fact that the takedown notices contained fair use analyses – even if those analyses were identical and pro forma – seemed to satisfy the requirement to “consider” fair use before issuing a takedown notice as required by the Ninth Circuit's 2016 Lenz decision. And the court noted the Ninth Circuit had held that a jury must determine whether the defendant's actions were sufficient to form a subjective good faith belief about the allegedly infringing content's fair use or lack thereof.³⁹³³

Accordingly, the court ruled that, because it is generally a factual issue whether the analysis that the defendant did conduct of the alleged infringing material was sufficient, it necessarily follows that to plead a claim under Section 512(f), it is enough for the plaintiff to allege that the defendant did not consider fair use (sufficiently or at all) before issuing its takedown notices. And that is exactly what the plaintiff had alleged here. Requiring the plaintiff to allege more would effectively impose a heightened pleading standard, and no authority had held that claims under Section 512(f) must be pleaded with particularity under Fed. R. Civ. P. 9(b). The court therefore concluded that, although it might be advisable for a plaintiff to aver additional facts (such as its own analysis of fair use) to support the allegation that a defendant's fair use analysis was merely pro forma, the court could not conclude that the plaintiff was required to plead such facts in order to state a plausible claim under Section 512(f).³⁹³⁴

(xxx) Warner Records v. Charter Communications

The background of this case is described in Section III.C.5(d) above. The defendants asserted a counterclaim under Section 512(f) based on the fact that the plaintiffs' original complaint identified 11,482 works that were claimed to have been infringed by Charter's subscribers, whereas their First Amended Complaint identified only 11,027 allegedly infringed works. Charter argued that the fact the First Amended Complaint identified 455 fewer works implied that the plaintiffs dropped those works because they did not have valid infringement

³⁹³² ENTTech Media Grp. LLC v. Okularity, Inc., 2021 U.S. Dist. LEXIS 45118 at *9, *11 (C.D. Cal. Mar. 10, 2021).

³⁹³³ Id. at *11-12.

³⁹³⁴ Id. at *13-14.

claims as to them. That, in turn, was an alleged “misrepresentation” that supported a claim for damages under Section 512(f).³⁹³⁵

The court rejected this claim, finding that Charter had not alleged facts plausibly showing that the plaintiffs knowingly or materially misrepresented their infringement claims in the original complaint. The closest the Section 512(f) counterclaim came to alleging a knowing misrepresentation was in a paragraph that asserted that “at all times, Plaintiffs had or should have had knowledge of the status of their purposed ownership or control of copyrights when they sent infringement notices regarding those copyrights, including those at issue in this case.” That conclusory statement, based on information and belief, and sounding in language of negligence, fell short of the mark. And in any event, the court found that 455 of 11,482 works was immaterial, representing slightly less than 4% of the total. The court also found it significant that the plaintiffs dropped works as to which they allegedly determined that they did not have a valid claim, and noted it would be ironic that an amendment to reduce the number of infringed works would support a counterclaim. Finally, the court found that Charter had not alleged that it incurred damages as the result of relying on the misrepresentation in removing or disabling access to the material or activity claimed to be infringing. It was undisputed that although Charter had notified some of its subscribers of some of the plaintiffs’ claims of infringement, it had not cancelled any subscriptions or taken other actions to disable subscribers’ access to Charter’s services. Accordingly, the court granted the plaintiffs’ motion to dismiss the Section 512(f) counterclaim.³⁹³⁶

(xxxi) The Sunny Factory v. Chen

In this case, the defendants – who were lawyers – issued several takedown notices to Amazon reporting that their client’s copyright was being infringed by products distributed by the plaintiff through Amazon. In response, Amazon stopped the sale of the plaintiff’s products. The plaintiff sued under Section 512(f). The court noted that the plaintiff had not alleged sufficient facts to support its allegation that the defendants made knowing material misstatements repeatedly to Amazon for the purpose of stifling competition. In response, the plaintiff cited Section 512(g)(2)(C), which conditions the safe harbor for a service provider against liability for removal of a work in response to a notice of claimed infringement on the requirement that the service provider replace the removed material in not less than 10, nor more than 14, business days following receipt of a counter notice, unless it first receives notice from the submitter of the takedown notice that it has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity. The plaintiff argued based on Section 512(g)(2)(C) that the filing by defendants of repeated claims for copyright infringement without filing a claim in court demonstrated that they acted in bad faith. The court rejected this argument, ruling that Section 512(g)(2)(C) does not impose a requirement on a submitter of notices of claimed infringement,

³⁹³⁵ Warner Records Inc. v. Charter Communs., Inc., 2020 U.S. Dist. LEXIS 206702 at *8-9 (D. Colo. Nov. 5, 2020).

³⁹³⁶ Id. at *9-11.

but rather provides an exception to liability for a service provider's good faith disabling of access to material. Accordingly, the court dismissed the plaintiff's Section 512(f) claim.³⁹³⁷

(xxxii) Business Casual Holdings v. TV-Novosti

The plaintiff submitted a takedown notice to YouTube, in response to which YouTube took down the allegedly infringing material. The defendant submitted a counter notification, in response to which YouTube informed the plaintiff that it would restore the material if the plaintiff did not seek a court order to restrain the allegedly infringing activity within 10 business days. In response, the plaintiff filed a lawsuit, causing YouTube not to restore the material. The plaintiff's complaint included claims for both copyright infringement and filing of a false counter notification. The defendant moved to dismiss the DMCA claim on the ground that the plaintiff had not alleged that YouTube in fact ceased to disable access to the defendant's videos. The court rejected the defendant's argument, holding that Section 512(f), read in the context of the section as a whole, is not limited only to cases where the service provider actually ceases to disable access to the allegedly infringing material, but also applies where the service provider only threatens to do so.³⁹³⁸

The court further noted that the plaintiff had not alleged that the allegedly infringing videos were ever restored to YouTube, and neither party had cited any authority for the proposition of whether the filing of a bad faith counter notification that does not trigger a service provider to cease or disable access to allegedly infringing material is sufficient to trigger liability under Section 512(f). By its terms, Section 512(f) applies only when there has been a misrepresentation in the counter notification and the service provider relies on that misrepresentation and ceases to disable access to the allegedly infringing material. The court ruled, however, that given the cursory nature of the parties' briefs, the parties were welcome to develop the factual and legal record of whether there are remedies for the filing of unsuccessful bad faith counter notifications, but they should do so in the context of an amended complaint. Accordingly, the court granted the motion to dismiss the DMCA claims without prejudice to the assertion of an amended DMCA claim in an amended complaint.³⁹³⁹

(5) Filing of False DMCA Counter notices – Section 512(g)(3)(C)

(i) Hosseinzadeh v. Klein

In this case the plaintiff was a filmmaker who posted an original video on YouTube referred to by the court as the "Hoss video." The defendant posted a video on YouTube, referred to as the "Klein video," in which the defendants commented on and criticized the Hoss video, interspersing relatively short segments of the Hoss video with long segments of commentary, ultimately using three minutes and fifteen seconds of the five minute, twenty-four

³⁹³⁷ The Sunny Factory, LLC v. Chen, 2022 U.S. Dist. LEXIS 43969 at *1, *12-13 (N.D. Ill. Mar. 11, 2022).

³⁹³⁸ Business Casual Holdings, LLC v. TV-Novosti, 2022 U.S. Dist. LEXIS 45283 at *6-7, *13 (S.D.N.Y. Mar. 14, 2022).

³⁹³⁹ Id. at *14-15.

second long Hoss video. The plaintiff submitted a DMCA takedown notice to YouTube regarding the Klein video and YouTube took it down the same day. The defendants submitted a DMCA counternotice challenging the takedown on the basis that the Klein video was fair use and non-commercial. Three days later, the plaintiff filed suit alleging the defendants infringed the plaintiff's copyrights and made misrepresentations in a counternotice in violation of Section 512(g)(3)(C) of the DMCA.³⁹⁴⁰

The court first found that the defendant's video was a fair use, and then turned to the plaintiff's claim for misrepresentations in the defendant's counternotice. The court noted the Ninth Circuit's requirement that, in submitting a takedown notice, a copyright holder must form a subjective good faith belief that a use is not authorized. Thus, a copyright holder is not liable for misrepresentation under the DMCA if it subjectively believes the identified material infringes its copyright, even if that belief is ultimately mistaken. The court ruled that the same subjective standard should apply to the "good faith belief" requirement for counternotices. If the same standard did not apply, creators of allegedly infringing work would face a disparate and inequitable burden in appealing an online service provider's decision to remove or disable access to their work.³⁹⁴¹

In view of the court's ruling of fair use, the court noted that the claim the defendants made misrepresentations in their counternotice must also be dismissed because the defendants' representation that the Klein video was fair use was factually accurate. But the court went on to note that, even if the Klein video was not fair use, the court would still dismiss the misrepresentation claim because the defendants clearly had a subjective good faith belief that their video did not infringe the plaintiff's copyrights. It was undisputed that the defendants understood the concept of fair use and had an established practice for ensuring their videos made fair use of copyrighted material. It was also undisputed the defendants filed a counternotice alleging that the Klein video constituted fair use. That undisputed evidence clearly established the subjective good faith belief required under Section 512(g)(3)(C). The plaintiff had failed to proffer any evidence suggesting the defendants lacked a subjective good faith belief, and therefore failed to create a triable issue. Accordingly, the court dismissed the misrepresentation claim.³⁹⁴²

(6) Other Provisions

Section 512(g) provides that a Service Provider shall not be liable for the good faith disabling of access to or removal of material or activity claimed to be, or appearing from the facts and circumstances to be, infringing (regardless of whether the material or activity is ultimately determined to be infringing). However, if such removal is taken pursuant to a notice given to the Service Provider pursuant to the provisions of the third safe harbor (which will be referred to herein as the "safe harbor notice"), then Section 512(g)'s limit on liability is

³⁹⁴⁰ Hosseinzadeh v. Klein, 276 F. Supp. 3d 34, 39-40 (S.D.N.Y. 2017).

³⁹⁴¹ Id. at 44-45.

³⁹⁴² Id. at 47.

conditioned upon compliance with the following. The Service Provider must (i) take reasonable steps to promptly notify the subscriber that it has removed or disabled access to the subscriber's allegedly infringing material; (ii) upon receipt of a counter notification from the subscriber stating under penalty of perjury that it has a good faith belief that the materials were removed or disabled as a result of mistake or misidentification of the material, provide the person who submitted the safe harbor notice with a copy of the counter notification and inform that person that the Service Provider will replace the removed material or cease disabling access to it in ten business days; and (iii) replace the removed material and cease disabling access to it not less than ten, nor more than fourteen, business days following receipt of the counter notification, unless the Service Provider receives notice from the person submitting the safe harbor notice that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the Service Provider's system.

As described in more detail in Section II.G.6(h) above, Section 512(h) sets up a procedure through which a copyright owner may obtain an order through a United States district court directing the Service Provider to release the identity of an alleged direct infringer acting through the Service Provider's system or network.

Under Section 512(l), failure of a Service Provider to fit into one of the safe harbors does not affect the Service Provider's claim that its conduct is nonetheless noninfringing, or any other defense.

Finally, Section 512(m) clarifies that the safe harbors are not conditioned upon a requirement that the Service Provider monitor its system for infringements, or access, remove or disable access to material where such conduct is prohibited by law (for example, by the Electronic Communications Privacy Act).

(7) Injunctions Against Service Providers

Under Section 512(j), if a Service Provider is subject to injunctive relief other than under the first safe harbor, courts are limited to injunctions that restrain the Service Provider from providing access to infringing material at particular online sites on its service, that restrain it from providing services to a subscriber engaging in infringing activity by terminating the subscriber, or that otherwise are "necessary to prevent or restrain infringement of specified copyrighted material at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose." If the Service Provider is subject to injunctive relief under the first safe harbor, then courts are limited to injunctions that restrain the Service Provider from providing access to a subscriber engaging in infringing activity by terminating the subscriber or by taking reasonable steps specified in the order to block access to a specific, identified, online location outside the United States.

(8) Designation of Agent to Receive Notification of Claimed Infringement

To take advantage of the third safe harbor for innocent storage of infringing information, Section 512(c)(2) requires a Service Provider to designate an agent to receive notifications of

claimed infringement by providing contact information for that agent to the Copyright Office and through the Service Provider's publicly accessible website. Failure to do so makes a service provider ineligible for the safe harbors.³⁹⁴³ Section 512(c)(2) requires the Copyright Office to maintain a current directory of designated agents and to make the listing available to the public.

On Nov. 3, 1998, the Copyright Office published interim regulations for the designation of such agents.³⁹⁴⁴ Because the DMCA was made effective immediately, the Copyright Office did not have time to conduct rulemaking proceedings. Accordingly, the Office adopted interim regulations, and stated its intent in the next several weeks to publish a notice of proposed rulemaking to seek comments on more comprehensive final regulations governing the designation of agents to receive notification of claimed infringement. Upon the adoption of final rules, Service Providers would have to file new designations that satisfy the requirements of the final regulations.³⁹⁴⁵

Under the Copyright Office's interim rules, the Office did not provide printed forms for filing interim designations of agents. Instead, Service Providers were required to file a document entitled "Interim Designation of Agent to Receive Notifications of Claimed Infringement," identified as such by a prominent caption or heading. The Interim Designation, which required a filing fee of \$20, was required to contain the following information: (i) the full legal name and address of the Service Provider; (ii) all names under which the Service Provider is doing business; (iii) the name, full address, telephone number, facsimile number, and electronic mail address of the agent to receive notification of claimed infringement; and (iv) the signature of the appropriate officer or representative of the Service Provider designating the agent, together with the printed name and title of the person signing the designation, and the date of signature.³⁹⁴⁶

In 2016, the Copyright Office shifted to a new electronic system for designation of agents. On Nov. 1, 2016, the Copyright Office adopted a final rule governing the designation and maintenance of DMCA agent information under its new electronic system.³⁹⁴⁷ On May 10, 2017, the Copyright Office issued non-substantive technical amendments to its regulations governing the submission of designated agent and service provider information pursuant to the DMCA.³⁹⁴⁸ Instructions for designation of an agent through the Copyright Office's online registration system may be found at <https://www.copyright.gov/dmca-directory/>, and FAQs may be found at

³⁹⁴³ See, e.g., *Van Stry v. McCrea*, 2020 U.S. Dist. LEXIS 62338 at *15-17 (plaintiff granted summary judgment that the defendant was not entitled to the Section 512(c) safe harbor because there was no dispute that the defendant failed to designate an agent with the Copyright Office to receive notifications of claimed infringement, despite the fact that the plaintiff's counsel was otherwise able to find a valid contact address for sending a notification of infringement).

³⁹⁴⁴ 63 Fed. Reg. 59233 (Nov. 3, 1998).

³⁹⁴⁵ *Id.* at 59234.

³⁹⁴⁶ *Id.* at 59234-35.

³⁹⁴⁷ 81 Fed. Reg. 75695 (Nov. 1, 2016).

³⁹⁴⁸ 82 Fed. Reg. 21696 (May 10, 2017).

<https://www.copyright.gov/dmca-directory/faq.html>. The DMCA Designated Agent Directory may be searched at <https://dmca.copyright.gov/osp/>. An index of the Directory may be found at <https://www.copyright.gov/onlinesp/list/index.html>.

(i) CoStar v. Loopnet

In CoStar Group Inc. v. LoopNet, Inc.,³⁹⁴⁹ the court ruled that the safe harbor could not protect LoopNet for any alleged infringements taking place before December 8, 1999, the date that LoopNet designated an agent to receive notifications of claimed infringement under the DMCA, as required by Section 512(c)(2) of the DMCA.³⁹⁵⁰

(ii) Wolk v. Kodak Imaging Network

In Wolk v. Kodak Imaging Network, Inc.,³⁹⁵¹ the plaintiff had submitted various notices to Photobucket requesting that images infringing her copyrights be taken down, some of which complied with the DMCA notice requirements and some of which did not. Where a DMCA compliant notice was submitted, Photobucket took down the allegedly infringing photo. Photobucket also had taken down photos where the plaintiff had sufficiently identified the alleged infringements, even if the notice was not DMCA compliant. Despite these removals, the plaintiff contended that more infringing photos remained on Photobucket, although she had not provided DMCA compliant notices to remove them.³⁹⁵²

Photobucket sought summary judgment under the DMCA safe harbors. For purposes of asserting the safe harbors as a defense, the court ruled that Photobucket had adequately satisfied the predicate requirement of designating an agent to receive DMCA notifications. Photobucket posted contact information of its agent on its web site, including instructions to send notices to “Copyright Agent” at a listed physical address, email address, or fax. The court held that, although this contact information did not include a name or phone number, the statute mandates that the service provider provide only “substantially the following information” referenced in the statute, and by including the physical address, email address and fax number of the copyright agent, Photobucket had included sufficient information to have properly designated an agent.³⁹⁵³

³⁹⁴⁹ 164 F. Supp. 2d 688 (D. Md. 2001), aff’d, 373 F.3d 544 (4th Cir. 2004).

³⁹⁵⁰ Id. at 697 & n.4.

³⁹⁵¹ 2011 U.S. Dist. LEXIS 27541 (S.D.N.Y. Mar. 17, 2011).

³⁹⁵² Id. at *1-2.

³⁹⁵³ Wolk v. Kodak Imaging Network, Inc., 840 F. Supp. 2d 724, 748-49 (S.D.N.Y. 2012), aff’d sub nom. Wolk v. Photobucket, Inc., 569 Fed. Appx. 51 (2d Cir. 2014) (summary order).

(iii) Perfect 10 v. Yandex

In Perfect 10, Inc. v. Yandex,³⁹⁵⁴ Yandex offered a broad range of search functions over the Internet. Perfect 10 sent hundreds of DMCA takedown notices to Yandex requesting that it remove links to thousands of allegedly infringing images. Perfect 10 moved for partial summary judgment, among other things, that Yandex was ineligible for any DMCA safe harbor defense during the period when it had no DMCA agent registered with the Copyright Office. The court granted Perfect 10 partial summary judgment on the issue. The court rejected Yandex's argument that Section 512(c)(2) does not require that its agent be registered with the Copyright Office, only that it have an agent, on the ground that Congress intended for the courts to enforce only substantial compliance with the DMCA's safe harbor requirements. The court noted that the phrase "substantially the following information" in the statutory provision requiring registration of an agent modifies the ensuing subparagraphs that list types of contact information for an agent, and does not excuse a failure to provide the Copyright Office with any information at all.³⁹⁵⁵

(iv) Oppenheimer v. Allvoices

In this case, the plaintiff brought claims for copyright infringement for unlicensed use of his photographs on the defendant Allvoices' web site. Allvoices was an online service provider that operated a web site set up as a community for its users to share and discuss news, by contributing related text, video and images, and commenting. Citizen journalists who posted news, videos, images and commentary were paid consideration for their article contributions based on the popularity of, and web traffic to, their articles. Allvoices filed a motion to dismiss in part based on the Section 512(c) safe harbor. Several of the plaintiffs' photographs were posted to the web site around January 7, 2011, but Allvoices did not designate a DMCA-related copyright agent with the Copyright Office until March 15, 2011. The court ruled that Allvoices could not invoke the safe harbor of Section 512(c)(1) with respect to infringing conduct that occurred before it designated a DMCA-related agent with the Copyright Office. However, the court noted that it remained unresolved whether Allvoices' potential liability in the case was limited to the time between when the plaintiff's works were posted and March 15, 2011. The parties had not presented this issue to the court and so the court refused to address it.³⁹⁵⁶

(v) BWP Media v. Hollywood Fan Sites

In this case, the plaintiffs were the owners of photos of celebrities that they alleged appeared without a license on web sites operated by the defendants. The plaintiffs brought a motion to strike the defendants' affirmative safe harbor defense because of failure to satisfy the designation of agent requirement. The defendants were each subsidiaries of Hollywood.com, LLC. One of them, Fan Sites Org, LLC, had submitted its designation of agent to the Copyright

³⁹⁵⁴ 2013 U.S. Dist. LEXIS 65802 (N.D. Cal. May 7, 2013).

³⁹⁵⁵ Id. at *19-21.

³⁹⁵⁶ Oppenheimer v. Allvoices, Inc., 2014 U.S. Dist. LEXIS 80320 at *1-2, *15-18 (N.D. Cal. June 10, 2014).

Office after the earliest infringing acts alleged by the plaintiffs and did not contest that it would be barred from asserting the safe harbor for any infringement shown to have occurred before the date of its designation of agent.³⁹⁵⁷

The other subsidiary, Hollywood Fan Sites LLC (HFS), asserted that, although a designation of agent in its name was also filed after the earliest infringing acts alleged by the plaintiffs, it was covered by an earlier designation of agent filed by its parent Hollywood.com, LLC in 2008. The court rejected this argument, noting that there was nothing in the 2008 designation that could be interpreted to make any reference to HFS. The portion of the designation form for full legal name of the service provider listed only the name “Hollywood.com, LLC” and the alternative names field listed only “Hollywood.com” and “Media By Numbers,” both of which were alternate names for Hollywood.com, LLC. The court concluded that the statute does not contemplate that a service provider entity can be shielded by the safe harbor where that entity has no presence at all in the directory of designated agents of the Copyright Office. The court found it implausible that parties attempting to find a service provider’s DMCA agent designation using the Copyright Office database could be expected to have independent knowledge of the corporate structure of a particular service provider.³⁹⁵⁸

The court also stated that, even had the 2008 designation indicated that it was intended to cover HFS, it is far from clear that a single designation can cover multiple entities, noting that the Copyright Office’s interim regulations for designation of agents stated, “During the interim period before final regulations are promulgated, each Interim Declaration may be filed only on behalf of a single service provider.” Accordingly, the court ruled that the two subsidiaries were barred from asserting the safe harbor as a defense to any infringement occurring before the date of filing of their individual designation of agent forms with the Copyright Office.³⁹⁵⁹

(vi) **Van Stry v. McCrea**

In this case the defendant, who asserted the Section 512(c) safe harbor, failed to register a designated agent with the Copyright Office. The court ruled that this failure precluded the defendant from benefit of the safe harbor, rejecting his argument that the registered agent requirement was irrelevant in this case because the plaintiff’s counsel was able to find a valid contact address for the plaintiff and submit a takedown notice. The court ruled that the statute expressly requires the designated agent to be listed in the Copyright Office’s directory, even if that information is available elsewhere.³⁹⁶⁰

³⁹⁵⁷ BWP Media USA Inc. v. Hollywood Fan Sites LLC, 115 F. Supp. 3d 397, 397-98, 401 (S.D.N.Y. 2015).

³⁹⁵⁸ Id. at 401-02.

³⁹⁵⁹ Id. at 402-04.

³⁹⁶⁰ Van Stry v. McCrea, 202 U.S. Dist. LEXIS 62338 at *15-17 (E.D. Tex. Apr. 9, 2020).

(9) Whether the Safe Harbors Apply to Pre-1972 Sound Recordings

Before passage of the Orrin G. Hatch-Bob Goodlatte Music Modernization Act (MMA), Public Law 115-264, 132 Stat. 3676 (2018), the federal courts had reached contrary conclusions on the issue whether the DMCA safe harbors apply to claims of infringement against service providers with respect to sound recordings fixed prior to February 15, 1972, the date on which sound recordings first became eligible for federal copyright protection (referred to herein as pre-1972 sound recordings). As summarized in subsections (i) and (ii) below, a majority of courts eventually concluded that the safe harbors do apply to pre-1972 sound recordings.

Title I of the MMA, called the Musical Works Modernization Act (MWMA) and codified at 17 U.S.C. § 1401, provides that the DMCA safe harbors do apply to pre-1972 sound recordings. Specifically, 17 U.S.C. § 1401(f)(3) provides, “The limitations on actions described in section 507 shall apply to a claim under subsection (a) with respect to a sound recording fixed before February 15, 1972.” The referenced subsection (a) prohibits engaging without the consent of the rights owner in activity covered by the MWMA (i.e., digital phonorecord deliveries in the form of permanent downloads, limited downloads, and interactive streams) with respect to pre-1972 sound recordings, and affords the copyright remedies provided in Sections 502-505 and 1203 to the same extent as an infringer of copyright or a person that engages in unauthorized activity under Chapter 12. Section 1401(e)(1) preempts most claims of common law copyright or equivalent right under laws of any state arising from a digital audio transmission or reproduction that was made before the effective date of the MMA of a pre-1972 sound recording.

(i) Cases Concluding the Safe Harbors Apply to Pre-1972 Sound Recordings

Before passage of the MMA, a majority of federal court decisions ultimately concluded that the DMCA safe harbors apply to claims of infringement against service providers with respect to sound recordings fixed prior to February 15, 1972. The first was Capitol Records, Inc. v. MP3Tunes, LLC,³⁹⁶¹ for the reasons discussed in Section III.C.6(b)(1)(iii).t above. The second was UMG Recordings, Inc. v. Escape Media Group, Inc.,³⁹⁶² largely on the grounds of the persuasiveness of the reasoning of the MP3Tunes decision.³⁹⁶³

The federal district court in Capitol Records, LLC v. Vimeo, LLC³⁹⁶⁴ reached the opposite conclusion for reasons similar to the New York state court’s decision in UMG Recordings v. Escape Media (discussed in the next subsection) and a December 2011 report from the Copyright Office concluding the DMCA safe harbors do not apply to pre-1972 recordings.³⁹⁶⁵ The

³⁹⁶¹ 821 F. Supp. 2d 627 (S.D.N.Y. 2011).

³⁹⁶² 2012 N.Y. Misc. LEXIS 3214 (S.Ct. N.Y. July 10, 2012).

³⁹⁶³ Id. at *3-12.

³⁹⁶⁴ 972 F. Supp. 2d 500 (S.D.N.Y. 2013), rev’d, 2016 U.S. App. LEXIS 10884 (2d Cir. June 16, 2016)..

³⁹⁶⁵ Federal Copyright Protection for Pre-1972 Sound Recordings (Dec. 2011), available at www.copyright.gov/docs/sound/pre-72-report.pdf.

court shared the view articulated in the Copyright Office report that “it is for Congress, not the courts, to extend the Copyright Act to pre-1972 sound recordings, both with respect to the rights granted under the Act and the limitations on those rights (such as *section 512*) set forth in the Act.”³⁹⁶⁶ However, the court certified the issue for interlocutory appeal to the Second Circuit.³⁹⁶⁷

On interlocutory appeal, the Second Circuit reversed in an opinion by Judge Leval.³⁹⁶⁸ The Second Circuit criticized the Copyright Office’s reasoning in its December 2011 report. The court noted that the 2011 report arrived at its conclusion that Section 512(c)’s safe harbor applies only to post-1972 sound recordings by the following reasoning. The term “infringement of copyright” employed in Section 512(c) is defined in Section 501(a) as the violation of any of the exclusive rights of the copyright owner provided by Sections 106 through 122. Therefore, that term, when used in Section 512(c), refers only to infringement of rights protected under Title 17 and does not include infringement of rights protected under state law. The Second Circuit disagreed with this reasoning. The court noted that Section 501(a) does not contain such a definition of “infringement of copyright,” nor does Section 501(a) purport to define “infringement of copyright.” Rather, Section 501(a) provides, “Anyone who violates any of the exclusive rights of the copyright owner as provided by *sections 106 through 122* ... is an infringer of the copyright.” The Second Circuit reasoned that the statement that one who violates rights identified in specified sections is an “infringer of copyright” does not purport to set forth an exclusive definition of “infringer of copyright” and therefore is not incompatible with interpreting the safe harbor to apply to infringement of state copyright laws. The court also noted that within the provisions of the copyright statute, infringements are specified that are not among those specified in Sections 106-122, such as infringement of vessel hull designs in Section 1309.³⁹⁶⁹

The court found that a literal and natural reading of Section 512(c) leads to the conclusion that its use of the phrase “infringement of copyright” *does* include infringement of state laws of copyright. In this instance, Congress did not qualify the phrase “infringement of copyright” by adding, as it did in other sections of the statute, the words “under this title.” The court also found good reasons to believe that Congress meant to cover all types of copyright infringement. To construe Section 512(c) as leaving service providers subject to liability under state copyright laws for postings by users of infringements of which the service providers were unaware would defeat the very purpose Congress sought to achieve in passing the safe harbors. Service providers would be compelled either to incur heavy costs of monitoring every posting to be sure it did not contain infringing pre-1972 recordings, or incurring potentially crushing liabilities under state copyright laws (noting that some of the most popular recorded music of all

³⁹⁶⁶ Vimeo, 972 F. Supp. 2d at 536-37 (quoting the Copyright Office report at 132).

³⁹⁶⁷ Capitol Records, LLC v. Vimeo, LLC, 972 F. Supp. 2d 537, 556 (S.D.N.Y. 2013), aff’d, 2016 U.S. App. LEXIS 10884 (2d Cir. June 16, 2016).

³⁹⁶⁸ Capitol Records, LLC v. Vimeo, LLC, 2016 U.S. App. LEXIS 10884 (2d Cir. June 16, 2016).

³⁹⁶⁹ Id. at *26-28.

time was recorded before 1972, including The Beatles, The Supremes, Elvis Presley, Aretha Franklin, Barbra Streisand, and Marvin Gaye). The court found the financial burdens in either case would be substantial and would likely either dissuade service providers from making large investments in the expansion of the growth and speed of the Internet (which Congress sought to encourage) or perhaps cause them to charge so much for the service as to undermine substantially the public usefulness of the service Congress undertook to promote.³⁹⁷⁰

Accordingly, the court vacated the district court's grant of summary judgment to the plaintiffs as to the availability to Vimeo of the DMCA safe harbor in relation to liability for infringement of pre-1972 sound recordings.³⁹⁷¹ Over the following months, the parties briefed new and renewed motions in view of the Second Circuit's decision. One such motion brought by Vimeo was to dismiss the plaintiff's unfair competition claims on the ground that they fell within the DMCA safe harbor. The Second Circuit had held that the safe harbor applies equally to copyright infringement claims under state and federal law. The question for the district court was whether the safe harbor also can apply to non-copyright claims that are founded on copyright infringement. The court ruled in the affirmative. In the same way that the statute does not distinguish between federal and state copyright infringement claims, it does not distinguish between copyright infringement claims and other types of claims that result in liability for infringement of copyright. Instead, the safe harbor precludes liability for a particular type of conduct – namely, infringement of copyright. Whenever copyright infringement is a necessary element of a claim, liability for that claim amounts to liability for infringement of copyright under the DMCA because no liability could be imposed absent the relevant copyright infringement. Accordingly, the court concluded that claims for unfair competition under New York law fall within the safe harbor when they are predicated on copyright infringement.³⁹⁷²

Here, the plaintiffs explicitly premised their unfair competition claims on Vimeo's (or its users') purported infringement of their copyrights to the pre-1972 recordings. They alleged no other misappropriation of property or underlying conduct on which they could base their unfair competition claims. Thus, if Vimeo was liable to the plaintiffs for unfair competition on the plaintiffs' theory, it would necessarily be liable for the infringement of copyright. The DMCA safe harbor therefore applied to the plaintiffs' unfair competition claims to the extent that Vimeo otherwise met the statute's requirements. The court observed that applying the DMCA safe harbor to unfair competition claims founded on copyright infringement would ensure that service providers are aware of the infringing activity that forms the basis for the claims brought against them. The court noted that often, and perhaps always, the DMCA analysis for establishing actual knowledge or red flag knowledge would go hand in hand with the unfair competition analysis for establishing bad faith, because it would be difficult to imagine a finding

³⁹⁷⁰ *Id.* at *28-30, *38. The Second Circuit also found unpersuasive the 2011 report's reliance on canons of statutory interpretation and found that the report misconstrued or misapplied some of the key case law on which it relied. *Id.* at *31-37.

³⁹⁷¹ *Id.* at *39-40.

³⁹⁷² *Capital Records, LLC v. Vimeo, LLC*, 2018 U.S. Dist. LEXIS 56049 at *3-4 & *9-10 (S.D.N.Y. Mar. 31, 2018).

of bad faith misappropriation of the plaintiffs' copyrights without some sort of awareness that the copyrights were being infringed.³⁹⁷³

The court granted Vimeo's motion to dismiss 273 of the plaintiffs' unfair competition claims for which the plaintiffs conceded that they failed to allege any red flag knowledge and, thus, necessarily fell within the DMCA safe harbor under the district court's (and the Second Circuit's) prior rulings in the cases.³⁹⁷⁴

(ii) Cases Concluding the Safe Harbors Do Not Apply to Pre-1972

Sound Recordings

As noted in the previous subsection, in 2013 the district court in Capitol Records, LLC v. Vimeo, LLC³⁹⁷⁵ reached the conclusion that the safe harbors do not apply to pre-1972 sound recordings, but the Second Circuit reversed that holding in a decision on an interlocutory appeal.

Also in 2013, a New York state court in the case of UMG Recordings, Inc. v. Escape Media Group, Inc.³⁹⁷⁶ concluded (contrary to the federal district court's ruling in a case between the same parties, as noted in the previous subsection) that the DMCA safe harbors don't apply to works protected under state copyright laws:

Initially, it is clear to us that the DMCA, if interpreted in the manner favored by defendant, would directly violate *section 301(c)* of the Copyright Act. Had the DMCA never been enacted, there would be no question that UMG could sue defendant in New York state courts to enforce its copyright in the pre-1972 recordings, as soon as it learned that one of the recordings had been posted on Grooveshark. However, were the DMCA to apply as defendant believes, that right to immediately commence an action would be eliminated. Indeed, the only remedy available to UMG would be service of a takedown notice on defendant. That is, at best, a limitation on UMG's rights, and an implicit modification of the plain language of *section 301(c)*. The word "limit" in 301(c) is unqualified, so defendant's argument that the DMCA does not contradict that section because UMG still retains the right to exploit its copyrights, to license them and to create derivative works, is without merit. Any material limitation, especially the elimination of the right to assert a common-law infringement claim, is violative of *section 301(c)* of the Copyright Act.³⁹⁷⁷

The court found no reason to conclude that Congress, in enacting the DMCA, recognized a limitation on common-law copyrights posed by the DMCA but intended to implicitly dilute

³⁹⁷³ Id. at *11-15.

³⁹⁷⁴ Id. at *16.

³⁹⁷⁵ 972 F. Supp. 2d 500 (S.D.N.Y. 2013).

³⁹⁷⁶ 2013 N.Y. App. Div. LEXIS 2642 (Apr. 23, 2013).

³⁹⁷⁷ Id. at *12-13. The court's rationale seems to ignore the fact that UMG could have sued the uploader of its copyrighted works.

Section 301(c) nonetheless. To the contrary, the court pointed out that the DMCA expressly identifies the rights conferred *by the Copyright Act* in stating who a “copyright infringer” is for purposes of the DMCA. The court reasoned that had Congress intended to extend the DMCA’s reach to holders of common-law rights it would have not provided so narrow a definition.³⁹⁷⁸

(10) Applicability of the Communications Decency Act to Pre-1972 Sound Recordings

The federal immunity afforded web sites under the Communications Decency Act (CDA) may apply to claims against web site operators under state copyright protection in pre-1972 sound recordings. In Perfect 10, Inc. v. CCBill LLC,³⁹⁷⁹ the Ninth Circuit made an important ruling with respect to Section 230 of the CDA, which states that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider,” and expressly preempts any state law to the contrary. 47 U.S.C. §§ 239(c)(1), (e)(3). The immunity created by Section 230(c)(1) is limited by Section 230(e)(2), which requires the court to “construe Section 230(c)(1) in a manner that would neither ‘limit or expand any law pertaining to intellectual property.’” Thus, Section 230 does not clothe service providers in immunity from “law[s] pertaining to intellectual property.” The CDA does not contain an express definition of “intellectual property.” The Ninth Circuit expressed the view that, “[b]ecause material on a website may be viewed across the Internet, and thus in more than one state at a time, permitting the reach of any particular state’s definition of intellectual property to dictate the contours of this federal immunity would be contrary to Congress’s expressed goal of insulating the development of the Internet from the various state-law regimes.”³⁹⁸⁰ Accordingly, the Ninth Circuit construed the term “intellectual property” to mean “federal intellectual property,” and concluded that the defendants were eligible for CDA immunity “for all of the state claims raised by Perfect 10.”³⁹⁸¹ Although the only state intellectual property claims the plaintiff had raised were trademark claims, the Ninth’s Circuit’s seemingly categorical ruling that Section 230’s immunity preempts all state intellectual property claims would presumably apply to state copyright law claims asserted against service providers.

7. Limitations of Liability of Online Service Providers under the Communications Decency Act

The Communications Decency Act (“CDA”), 47 U.S.C. § 230, was passed by Congress to create “a federal immunity to any *state law* cause of action that would hold computer service providers liable for information originating with a third party.”³⁹⁸² Specifically, 47 U.S.C. § 230(c)(1) provides that “[n]o provider or user of an interactive computer service shall be treated

³⁹⁷⁸ Id. at *13-14.

³⁹⁷⁹ 481 F.3d 751 (9th Cir. 2007), cert. denied, 552 U.S. 1062 (2007).

³⁹⁸⁰ Id. at 768.

³⁹⁸¹ Id.

³⁹⁸² Zeran v. America Online, 129 F.3d 327, 330 (4th Cir. 1997) (emphasis added).

as the publisher or speaker of any information provided by another information content provider.” Section 230(e)(3) provides in part that “[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.” One of the main purposes of the CDA immunity was to prevent service providers from being treated as the publisher of defamatory statements posted on or through the service by users.

(a) Stoner v. eBay

Stoner v. eBay Inc.³⁹⁸³ involved a novel application of the CDA to shield the online auction service provider eBay Inc. from liability under state laws for intellectual property infringements committed through its service. In that case, the plaintiff sought to hold eBay liable for the sale and distribution of illegal copies of sound recordings sold through its auction service, alleging that eBay’s participation in the same constituted unfair competition under the California Business and Professions Code § 17200 et seq. The court granted eBay’s motion for summary judgment, holding that the CDA’s immunity provisions shielded eBay from liability under the asserted state laws.

To establish immunity under the CDA, the court ruled that eBay had to establish the following three elements: “(1) that eBay is an interactive computer services provider; (2) that eBay is not an information content provider with respect to the disputed activity; and (3) that plaintiff seeks to hold eBay liable for information originating with a third-party user of its service.”³⁹⁸⁴ The parties did not dispute the first element – that eBay was an interactive computer services provider. The court ruled that eBay had established the second element because it was undisputed that the descriptions of the goods and services auctioned over the eBay service were created entirely by the sellers.³⁹⁸⁵

With respect to the third element, the plaintiff argued that the suit did not seek to hold eBay responsible for the publication of information provided by others, but rather for its own participation in selling contraband musical recordings by virtue of its charging fees and advertising for its services, providing insurance for all auctioned items, and providing escrow and payment services.³⁹⁸⁶ The court ruled that eBay’s role did not extend beyond the scope of the federal immunity:

A principle objective of the immunity provision is to encourage commerce over the Internet by ensuring that interactive computer service providers are not held responsible for how third parties use their services. ... To accomplish this objective, the immunity

³⁹⁸³ 56 U.S.P.Q.2d 1852 (Cal. Sup. Ct. 2000).

³⁹⁸⁴ Id. at 1853.

³⁹⁸⁵ Id.

³⁹⁸⁶ Id. at 1853-54.

extends beyond the publication of harmful material over the Internet, and encompasses the distribution of such material in transactions effected over the Internet.³⁹⁸⁷

The court noted that, at bottom, the plaintiff's contention was that eBay should be held responsible for failing to monitor the products auctioned over its service when it must have known that illicit recordings were being auctioned. The plaintiff argued that the very description of some recordings (e.g., "bootleg" tapes) identified them as contraband, so that by failing to intervene, eBay must be deemed to have knowingly joined in the unlawful sale.³⁹⁸⁸ The court rejected this argument:

Congress intended to remove any legal obligation of interactive computer service providers to attempt to identify or monitor the sale of such products. While such a service may be aware that a fraction of the large volume of data exchanged over its facilities involves unlawful activity, and might be able to detect a certain portion of those, the threat of liability for failing to monitor effectively would, in the judgment of Congress, deter companies such as eBay from making their service available as widely and as freely as possible. ... In order for liability to arise and the immunity to be lost, it would be necessary to show actual, rather than constructive, knowledge of illegal sales, and some affirmative action by the computer service, beyond making its facilities available in the normal manner, designed to accomplish the illegal sales.³⁹⁸⁹

Accordingly, the court granted eBay's motion for summary judgment. This case presents an additional weapon of immunity against liability for service providers, at least to the extent that claims are brought against the service provider under state law. Because many states have laws that may be asserted against service providers for infringement committed through their services – such as unfair competition laws and laws that protect sound recordings fixed before 1972 (when Congress added protection of sound recordings to the copyright statute) – the construction of the CDA under Stoner v. eBay, if followed by other courts, could provide a very useful grounds for immunity.

(b) Perfect 10 v. CCBill

The facts of Perfect 10, Inc. v. CCBill LLC³⁹⁹⁰ are set forth in Section III.C.6(b)(1)(i)d. above. In that case, Perfect 10 appealed rulings by the district court that CCBill and CWIE were immune from liability for state law unfair competition and false advertising claims based on the CDA. CCBill and CWIE cross appealed, arguing that the district court erred in holding that the CDA did not provide immunity against Perfect 10's right of publicity claims.³⁹⁹¹

³⁹⁸⁷ Id. at 1854.

³⁹⁸⁸ Id.

³⁹⁸⁹ Id. at 1855.

³⁹⁹⁰ 481 F.3d 751 (9th Cir. 2007), cert. denied, 552 U.S. 1062 (2007).

³⁹⁹¹ Id. at 757.

The Ninth Circuit noted that, although the CDA does not provide service providers with immunity from laws pertaining to intellectual property, it does not contain an express definition of “intellectual property.” Because state laws protecting intellectual property are not uniform, and because material on a website may be viewed across many states at a time, the court reasoned that permitting the reach of any particular state’s definition of intellectual property to dictate the contours of federal immunity under the CDA would be contrary to Congress’ expressed goal of insulating the development of the Internet from the various state-law regimes. Thus, in the absence of a definition from Congress, the court construed the term “intellectual property” in the CDA to mean “federal intellectual property.” Accordingly, CCBill and CWIE were eligible for CDA immunity for all of the state claims raised by Perfect 10.³⁹⁹²

8. Secondary Liability of Investors

(a) The Hummer Winblad/Bertelsmann Litigation

For a discussion of this litigation, see Section III.C.2(c)(8) above.

(b) UMG Recordings v. Veoh Networks

The plaintiffs, who owned rights to copyrighted sound recordings and musical compositions allegedly used without authorization by users submitting user-generated content to a site operated by Veoh Networks, sought to hold three of Veoh’s investors secondarily liable under theories of contributory liability, vicarious liability, and inducement of infringement. In UMG Recordings, Inc. v. Veoh Networks, Inc.,³⁹⁹³ in a decision designated not for publication, the court dismissed the plaintiff’s complaint with leave to amend. With respect to contributory liability, the court held that merely exercising ownership to select a Board of Directors cannot invite derivative liability.³⁹⁹⁴ “Nor is there a common law duty for investors (even ones who collectively control the Board) ‘to remove copyrighted content’ in light of the DMCA.”³⁹⁹⁵ The court distinguished the Hummer Winblad/Bertelsmann litigation on the ground that the court there upheld the complaints against the investors in view of the allegation that the investors had specifically ordered that infringing activity take place on the Napster site. With respect to vicarious liability, the court noted there was no direct financial benefit to Veoh’s investors in the form of fees from users or advertisers, and mere potential future increase in financial value of the investment was not sufficient. With respect to inducement to infringe, there was no allegation that the investors encouraged Veoh to infringe directly, thereby distinguishing the Grokster case.³⁹⁹⁶

³⁹⁹² Id. at 767-78.

³⁹⁹³ 2009 U.S. Dist. LEXIS 14955 (C.D. Cal. Feb. 2, 2009), aff’d sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011).

³⁹⁹⁴ Id. at *11.

³⁹⁹⁵ Id.

³⁹⁹⁶ Id. at *13-18.

On appeal, the Ninth Circuit affirmed. The plaintiffs argued that even if summary judgment was properly granted to Veoh on the basis of the DMCA safe harbor, the investors could remain potentially liable for their related indirect infringement because the district court did not make a finding regarding Veoh's direct infringement, and the investors did not qualify as services providers who could receive DMCA safe harbor protection. The Ninth Circuit noted that although it might seem illogical to impose greater liability on the investors than on Veoh itself, the court assumed without deciding that the suit against the investors could properly proceed even though Veoh was protected from monetary liability. Reaching the merits of the plaintiffs' secondary liability arguments, however, the court held that the district court properly dismissed the complaint against the investors.³⁹⁹⁷

With respect to contributory liability, the Ninth Circuit agreed with the district court that the plaintiffs had not alleged sufficiently that the investors gave material assistance in helping Veoh or its users accomplish infringement. The plaintiffs acknowledged that funding alone could not satisfy the material assistance requirement, but argued that the investors also directed the spending of the funding on basic operations including hardware, software and employees, which the plaintiffs argued formed the site and facilities for Veoh's direct infringement, analogizing to the Bertelsmann case. The court distinguished the Bertelsmann case, however, on the ground that the investor was Napster's only available source of funding and thus held significant power and control over Napster's operations. In this case, by contrast, there were multiple investors, and none of them could individually control Veoh.³⁹⁹⁸

The plaintiffs attempted to circumvent this distinction by arguing that the three investors together took control of Veoh's operations by obtaining three of Veoh's five board seats. The court noted that, even assuming that such joint control, not typically an element of contributory infringement, could satisfy the material assistance requirement, the complaint nowhere alleged that the investors agreed to work in concert. Although the complaint alleged that the investors sought and obtained board seats as a condition of their investments, the court noted that three investors individually acquiring one seat apiece was not the same as agreeing to operate as a unified entity to obtain and leverage majority control. Unless the three independent investors were on some level working in concert, then none of them actually had sufficient control over the board to direct Veoh in the way the plaintiffs contended. The court found this missing allegation to be critical because finding secondary liability without it would allow plaintiffs to sue any collection of directors making up 51% of the board on the theory that they constituted a majority, and therefore together controlled the company. In view of the missing allegations, the court affirmed the dismissal of the plaintiffs' contributory infringement claim.³⁹⁹⁹

Based on the same missing allegations, the court also affirmed the district court's dismissal of the plaintiffs' vicarious liability and inducement of infringement claims. The court noted that the plaintiffs' arguments that the investors distributed Veoh's services and had the

³⁹⁹⁷ UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022, 1045-46 (9th Cir. 2011).

³⁹⁹⁸ Id. at 1046.

³⁹⁹⁹ Id. at 1047.

right and ability to supervise the infringing users were premised on the same unalleged contention that the investors agreed to act in concert, and thus together they held a majority of seats on the board and maintained operational control over the company. Accordingly, the court affirmed the dismissal of the complaint against the investors.⁴⁰⁰⁰

9. Class Actions

In The Football Association Premier League Limited v. YouTube, Inc.,⁴⁰⁰¹ the court denied a motion for certification of a class action against YouTube and Google for infringements on YouTube of copyrighted material owned by The Football Association Premier League and a number of music publishers. The putative class consisted of “every person and entity in the world who own infringed copyrighted works, who have or will register them with the U.S. Copyright Office as required, whose works fall into either of two categories: they were the subject of prior infringement which was blocked by YouTube after notice, but suffered additional infringement through subsequent uploads (the ‘repeat infringement class’), or are musical compositions which defendants tracked, monetized or identified and allowed to be used without proper authorization (the ‘music publisher class’).”⁴⁰⁰² The court found the suggestion that a class action of the dimensions presented in the present case could be managed with judicial resourcefulness to be “flattering, but unrealistic.”⁴⁰⁰³ In Nov. 2013, the case was settled by stipulated dismissal.⁴⁰⁰⁴

D. Linking and Framing

The practice of “linking” is another activity that is ubiquitous on the World Wide Web. A “link” is an embedded electronic address that “points” to another Web location. Links may be of at least two different types. The first type, which will be referred to as an “outlink,” merely provides a vehicle by which a person browsing a Web page can go to another site by clicking on the link. The outlink stores the electronic address of the destination site, and clicking on the link sends that address to the browser, which in turn moves the user to the new destination site.

A second type of link, which will be referred to as an “inlink,” is a pointer to a document, image, audio clip or the like somewhere on the Web contained in another’s Web page which, in effect, pulls in the image, text or audio clip from the other Web page into the current document for display. In other words, a user looking at A’s Web page will see on that page image, text, or

⁴⁰⁰⁰ Id.

⁴⁰⁰¹ 2013 U.S. Dist. LEXIS 69401 (S.D.N.Y. May 15, 2013).

⁴⁰⁰² Id. at *6.

⁴⁰⁰³ Id. at *7-8.

⁴⁰⁰⁴ “UK Soccer League Ends Suit Against Google’s YouTube,” *Law360* (Nov. 13, 2013), available as of Nov. 15, 2013 at <http://www.wipo.int/export/sites/www/treaties/en/documents/pdf/hague.pdf>.

an audio clip that actually was “pulled in” from site owner *B*’s Web page.⁴⁰⁰⁵ When material from an inlink is displayed within the “frame” or window border of a page of the linking website, this type of linking is often referred to as “framing.”⁴⁰⁰⁶ The linking site is sometimes referred to as a “para-site,” with obvious pejorative connotations.

Both outlinks and inlinks raise a number of potential copyright issues. An outlink that points to a site containing infringing material may, for example, cause further infringing reproductions, public performances, public distributions, public displays, digital performances of sound recordings, and/or importations to occur when the user reaches that site and the infringing material is downloaded, imported and/or performed or displayed to the linking user. Even if material on the destination site is not infringing of its own right, the reproductions, distributions, and displays that occur as a result of the outlink may not be authorized, since the outlink may have been established (as is generally the case) without the explicit permission of the owner of material on the destination site. Under the WIPO treaties, the result of clicking on the outlink may be to generate an unauthorized access and transmission of the destination material. Or the outlink itself may be considered to be an unauthorized “making available to the public” of the material on the destination site – the owner of the destination site may wish to retain complete control of how and when information on its site is presented to the public.

It is unclear whether an outlink might also be considered the creation of an unauthorized derivative work. Viewed in one way, an outlink could be considered nothing more than a reference to another work, much like a citation in a law review article, that should not be considered a derivative work. One could argue that the material on the linked site is neither altered by the link nor “incorporated” into the linking site, but is seen in its original form when the user arrives there as a result of the link.

Viewed a different way, one could treat a site as a virtual collective work comprised of all material available to be viewed by the user in the course of browsing through the site. Links cause an “incorporation” – at least in a virtual sense – of the linked material into this collective work, thereby in some sense creating a derivative work. If the linked site material enhances the

⁴⁰⁰⁵ I. Trotter Hardy, “Computer RAM ‘Copies:’ Hit or Myth? Historical Perspectives on Caching As a Microcosm of Current Copyright Concerns,” 22 U. Dayton L. Rev. 423, 449 (1997). For example, “[a]n individual at the Massachusetts Institute of Technology for a while kept an inline link to the ‘Dilbert’ cartoon of the day. The cartoon appears on copyright owner United Media’s site, www.unitedmedia.com/comics/dilbert/, but to browser’s of the individual’s site, the cartoon appeared to be residing ‘there.’ United Media sent the individual, Dan Wallach, a ‘cease and desist’ letter, after which Wallach ceased and desisted the in-line linking.” *Id.* at 39 n.82.

⁴⁰⁰⁶ “Frame” technology is a page presentation capability available in both the Netscape Navigator and the Microsoft Internet Explorer browsers that enables the display of multiple, independently scrollable panels on a single screen. Frames may contain many types of elements, including text, hypertext, graphics, scrollable regions, and other frames.

value of the linking site, the linked site owner might argue that the linking site is “based upon” the linked site and therefore constitutes a derivative work.⁴⁰⁰⁷

The fair use or implied license doctrine may apply to many outlinks, because it is no doubt the case that many site owners will want their material disseminated as widely as possible, and references in to the site through links from other sites will be considered desirable. However, in some instances the linked site owner may argue that outlinks cause harm, and such harm should defeat a fair use or implied license defense. For example, nonconsensual links may result in burdensome amounts of traffic on the linked site from users the linked site is not targeting. The owner of the linked site could argue that such unwanted traffic prevents the owner from distributing copyrighted material on its site to its desired audience, thereby harming the potential market for its material. Alternatively, if the linking site is undesirable for some reason in the eyes of the linked site, the linked site might allege the linking diminishes the commercial value of its copyrighted material at the linked site. This might be the case, for example, if a site distributing pornographic material were to link to a religious site distributing religious material.⁴⁰⁰⁸

In addition to the issues of direct infringement discussed above, if a linked site contains infringing material, the link may give rise to contributory infringement on the part of the linking site, particularly if the linking site is promoting the copying, transmission, public display or public performance of material at the linked site. As noted in the previous Section, the SPA instituted a complaint against an OSP for contributory infringement based in part on the provision of links to Internet sites where unauthorized copies of the plaintiffs’ software could be found. Linking to a site containing infringing material may also give rise to vicarious liability, if the linking site derives financial benefit from the link.

As discussed in Section III.C.6(b) above, the DMCA provides a safe harbor under certain conditions to OSPs who set up outlinks to infringing material without knowledge of the infringement.

⁴⁰⁰⁷ “A ‘derivative work’ is a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted.” 17 U.S.C. § 101.

⁴⁰⁰⁸ Linking also raises a number of trademark issues. If the link consists of the linked site’s company name, trademark or logo, there is a danger of confusing site visitors about the source, affiliation or sponsorship of either the linking or the linked company’s goods or services. The language surrounding a link may also imply an endorsement by the linked company. For example, a list of links to “our many satisfied customers” states an endorsement by those customers of the linking site owner’s activities. From the opposite end, a linking site should carefully consider any explicit or implied endorsement it makes of the linked site’s goods or services over which it has no control. Linking to a site that contains defamatory material might make the linking entity itself liable as a “re-publisher” of the defamatory material by pointing users to the material. *See* Kopitzke, “Think Links: Web-Page Owners Should Consider Legal Consequences of Hypertext Links to Others’ Sites,” *San Francisco Daily Journal* (Dec. 20, 1996), at 5.

Inlinks may provide an even more direct basis for legal liability than outlinks. An inlink causes a reproduction of the linked material to be “pulled in” to the linking site, and therefore may cause an infringement of the right of reproduction, display, or performance, or may constitute the creation of an unauthorized derivative work, just as if material had been clipped from a printed source and placed in one’s own material. An inlink may also cause an infringing access or transmission of copyrighted material under the WIPO treaties.

Although beyond the scope of this paper, both outlinks and inlinks may raise issues of trademark infringement as well as copyright infringement. The trademarks of the linked site are often used as an icon on which the user may click to reach the linked site, and the trademark owner may argue that such use constitutes an infringement. In addition, both outlinks and inlinks may give rise to allegations of false implications of sponsorship or endorsement of the linking site by the company affiliated with the linked site or material, or of confusion as to source of the linked material.

There have been a number of cases challenging linking and framing on copyright grounds:⁴⁰⁰⁹

1. The Shetland Times Case

A case out of Scotland illustrates one type of harm that a linked site owner perceived to result from links to its site. In The Shetland Times Co., Ltd. v. Wills,⁴⁰¹⁰ the plaintiff, The Shetland Times (“Times”), maintained a website containing copies of articles that appeared in the printed version of its newspaper. Users visiting the site were initially presented with a “front page” containing headlines. Clicking on a headline linked the user to the full text of the article. The Times planned to sell advertising space on the front page.

The defendant, The Shetland News (“News”), also maintained a website. News took verbatim the headlines from Times’ site and placed them on News’ Web page to allow users at News’ site to link directly to the full text of Times’ articles, without having to first view Times’ front page. This bypassing of Times’ front page obviously caused harm to Times’ ability to sell advertising on the front page, since those readers of Times’ articles who arrived at the articles through links from News’ site would never see the ads. Times sued News in the Scotland Court of Sessions, alleging that News’ copying of Times’ headlines constituted copyright infringement.

The court issued an “interim edict” (a temporary order) pending a full hearing, ruling that the headlines could be considered copyrightable literary works. The court rejected the defendant’s argument that the headlines were not the product of sufficient skill or effort, finding

⁴⁰⁰⁹ In addition to the United States cases discussed in text, in Jan. 2001, an online European recruitment company, StepStone, obtained an injunction in Germany against OFiR, a Danish media group, preventing OFiR from deep linking (bypassing its home pages) to StepStone’s web site. The injunction was based on new European laws on database and copyright protection. Jean Eaglesham, “Recruiter Bans Rival’s Links,” available as of Jan. 18, 2001 at <http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT3YQ8AC2IC>.

⁴⁰¹⁰ Scotland Court of Session, Oct. 24, 1996.

that because many of the headlines consisted of eight or so words that imparted information, copying of the headlines might at least in some instances constitute copyright infringement.

The parties subsequently settled their dispute by agreeing that News would be permitted to link to stories on Times' website by means of headlines only in the following manner: each link to any individual story would be acknowledged by the legend "A Shetland Times Story" appearing underneath each headline and of the same or similar size as the headline; adjacent to any such headline or headlines there would appear a button showing legibly the Times masthead logo; and the legend and the button would each be hypertext links to the Times online headline page.

Under United States law, in most instances headlines will probably not be individually copyrightable under the "words and short phrases" doctrine,⁴⁰¹¹ which holds that individual words and short phrases such as titles are not copyrightable, although a collection of headlines might be copyrightable as a compilation. Thus, News' verbatim copying of a collection of Times' headlines from a single Times newspaper as a basis for News' links to the Times website might also constitute an infringement under United States copyright law. If Times' suit had been brought in the United States, News would no doubt argue that its use of the headlines was a fair use as part of news reporting.⁴⁰¹² Times would no doubt argue in response that the commercial harm to its advertising revenues from its headlines on its own front page should defeat News' fair use argument. Although it is unclear how such a case would be decided under United States fair use law, the case is a good illustration of the copyright issues that may arise out of the act of linking.

2. The Total News Case

In February of 1997, a number of news service providers (The Washington Post, Cable News Network, Times Mirror, Dow Jones and Reuters New Media) commenced a suit against Total News, Inc. ("Total News") and other defendants who were either providing website design and programming services to Total News or were principals of Total News. The case was the first to challenge framing as a copyright infringement.

The Total News website was a "para-site," designed to make over 1200 news sources from all over the world available at a single site. The Total News home page frame consisted of

⁴⁰¹¹ See, e.g., Hutchins v. Zoll Medical Corp., 492 F.3d 1377 (Fed. Cir. 2007) (copyright does not protect individual words and "fragmentary" phrases when removed from their form of presentation and compilation); Dobson v. NBA Properties, Inc., 1999 Copyr. L. Dec. ¶ 27,891 (S.D.N.Y. 1999) (phrase "Chicago Bulls Repeat Threepeat" was not protectable under the "words and short phrases doctrine" embodied in 37 C.F.R. § 202.1(a)); Acuff-Rose Music, Inc. v. Jostens, Inc., 988 F. Supp 289 (S.D.N.Y. 1997) (phrase "You've got to stand for something or you'll fall for anything" was an unprotectable cliché); Apple Computer, Inc. v. Microsoft Corp., 799 F. Supp. 1006 (N.D. Cal. 1992).

⁴⁰¹² "Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as ... news reporting ... is not an infringement of copyright." 17 U.S.C. § 107.

the totalnews.com URL at the top, a column of rectangular icons with the trademarked names of several of the plaintiffs running down the left margin, and advertising sold by the defendants at the bottom. At the right center portion of the screen was a news window. When the user first logged onto the Total News website, this window was occupied by a “compass” style array of hyperlinks to several of the plaintiffs’ websites. Clicking on the links would cause material from the plaintiffs’ websites to be displayed in the news window, but still within the Total News “frame.” Thus, for example, if a user clicked on the “Washington Post” link, the news window within the Total News frame would fill with an electronic version of *The Washington Post* newspaper linked in from *The Washington Post*’s own website. However, the totalnews.com URL would remain in place at the top of the frame and advertising sold by Total News would remain in place at the bottom of the frame.

Because the news window of the Total News frame was smaller than full screen in size,⁴⁰¹³ the effect of the framing by the defendants was to display only a portion of the original screens of material from the linked sites at any given time, and the user was forced to scroll the news window horizontally or vertically to see all of the original material from the linked sites. Thus, advertisements contained on the original pages of the linked sites were reduced in size, and in some cases were totally obscured by the Total News frame. At the same time, the user was continuously exposed to the advertising contained within the Total News frame:

Absent the “framing” by Defendants described above, someone wishing to view the content of Plaintiffs’ sites would, upon accessing those sites, see only Plaintiffs’ material as Plaintiffs intend for it to be seen. Use of Defendants’ website thus results in continuous, prolonged exposure to the logo, URL and advertising of totalnews.com. Defendants have promoted totalnews.com to advertisers and the public based entirely on Defendants’ ability to republish the content of Plaintiffs’ sites within the totalnews frames, including frames containing advertising.⁴⁰¹⁴

The plaintiffs alleged that Total News infringed the copyrights in various materials from the plaintiffs’ websites by “republishing” such material through the Total News site. The complaint did not state which specific rights of the copyright holders were infringed, referring instead merely to the plaintiff’s “exclusive rights under 17 U.S.C. § 106.”⁴⁰¹⁵ The plaintiffs also alleged claims for misappropriation of news, federal trademark dilution, federal and state trademark infringement, unfair competition, and tortious interference with contractual relations with their advertisers.

At least one of the plaintiffs, CNN, attempted to counteract the deleterious effects of the framing by employing special code in its Web page that checked to see if the content was being viewed from within a frame, and, if so, caused the unauthorized composite page to be replaced

⁴⁰¹³ The frame used by Total News to display its directory buttons took up slightly more than 15% of the page width. Gahtan, “Inappropriate Use of Frames May Constitute Infringement,” *Cyberspace Lawyer*, Apr. 1997, at 2, 2.

⁴⁰¹⁴ Complaint in *The Washington Post Co. v. Total News, Inc.*, 97 Civ. 1190 (S.D.N.Y. Feb. 20, 1997) at ¶ 35.

⁴⁰¹⁵ *Id.* ¶ 72.

with the CNN page on the entire screen. This technical solution had several problems, however. It took up to a minute or more to take effect, and a pop-up window inviting users to return to the Total News site was still able to appear superimposed on the CNN website.⁴⁰¹⁶

In June of 1997, the parties settled the case pursuant to a stipulated order of settlement and dismissal.⁴⁰¹⁷ Under the settlement, Total News agreed to stop framing the plaintiffs' websites. However, the settlement permitted Total News to maintain outlinks from the Total News website to any of the plaintiffs' websites, provided that the links were only via hyperlinks consisting of the names of the linked sites in plain text; Total News made no use, as hyperlinks or otherwise, of any of the plaintiffs' proprietary logos or other distinctive graphics, video or audio material; and the links were not likely to imply affiliation, endorsement or sponsorship by any plaintiff or otherwise cause confusion, dilution of the plaintiff's marks, or other violations of state or federal law.

3. The Seattle Sidewalk Case

In April of 1997, Ticketmaster Corporation brought an action in federal district court against Microsoft Corporation based on links from Microsoft's "Seattle Sidewalk" website to Ticketmaster's website. In February of 1998, Ticketmaster filed a Second Amended Complaint, which asserted claims for copyright and trademark infringement, as well as for unfair competition based on various common law and state law theories.

Ticketmaster maintained a website (www.ticketmaster.com) through which it sold and marketed tickets to various entertainment events. The "Seattle Sidewalk" site, one of a number of city guides maintained by Microsoft on The Microsoft Network, offered a guide to entertainment and restaurants available in the Seattle area. Microsoft placed links on the Seattle Sidewalk to the Ticketmaster site so that users of the Seattle Sidewalk could purchase tickets to events of interest online through Ticketmaster. Negotiations between Microsoft and Ticketmaster for an agreement allowing Microsoft to profit from linkage to and association with Ticketmaster's website failed, and Microsoft established the links – which in several instances bypassed the home page of the Ticketmaster site – without permission from Ticketmaster.

Ticketmaster sued Microsoft in federal court. With respect to its trademark claims, Ticketmaster asserted that the unauthorized links wrongfully appropriated, misused, and diluted Ticketmaster's name and trademarks. In particular, Ticketmaster noted in its complaint that it had a business relationship with MasterCard by which Ticketmaster had agreed to give MasterCard prominence over any other credit cards in any advertising. Ticketmaster objected to Microsoft's use of Ticketmaster's name in connection with MasterCard without giving MasterCard prominence. Ticketmaster also asserted that its name and trademark had been buried by Microsoft in metatag code at Microsoft's site in order to attract to Microsoft's

⁴⁰¹⁶ Gahtan, *supra* note 4013, at 4.

⁴⁰¹⁷ A copy of the Stipulation and Order of Settlement and Dismissal is available at www.callaw.com/opinions/hotdocs/totalnew.html.

Sidewalk websites Internet search engines and Internet users who were seeking information about tickets sold by and available through Ticketmaster. Ticketmaster alleged that this use of its name and trademark in metatags improperly feathered Microsoft's own nest at Ticketmaster's expense.

Ticketmaster also asserted claims of copyright infringement, based on the allegations that (i) in creating links to the Ticketmaster site, Microsoft repeatedly viewed and thus copied onto its own computers the copyrighted contents of Ticketmaster's website, and (ii) in the operation of the links, Microsoft was reproducing, publicly distributing and displaying without permission Ticketmaster's copyrighted website material.

In Microsoft's answer to Ticketmaster's complaint, Microsoft alleged that Ticketmaster could not complain about Microsoft's link to Ticketmaster's home page because Ticketmaster knew when it set up its website that owners of other Web pages would create such links. Microsoft noted that when an event required tickets, Microsoft routinely provided information about how to obtain them, including prices, telephone numbers and, where appropriate, hypertext links to relevant Web pages. Microsoft alleged that such information was freely available to the public and was not proprietary to Ticketmaster. Microsoft asserted numerous defenses, including (i) that Ticketmaster, when it chose to set up Web pages, assumed the risk that others would use its name and URLs; (ii) that Ticketmaster was estopped from complaining about Microsoft's link because Ticketmaster encouraged users to seek out its website and refer others to the site; and (iii) that Microsoft's presentation of information about Ticketmaster on its Seattle Sidewalk site was commercial speech protected by the First Amendment.⁴⁰¹⁸

Microsoft and Ticketmaster ultimately reached a settlement in the lawsuit, pursuant to which Microsoft was permitted to link to the Ticketmaster site, but not through links that bypassed Ticketmaster's home page.

4. The Futuredontics Case

In Sept. of 1997, Futuredontics, Inc., owner of a website relating to its dental referral service, filed a complaint against a defendant that was framing material from Futuredontics' website in the defendant's website.⁴⁰¹⁹ The frame displaying Futuredontics' website material included the defendant's logo, information on the defendant, and links to the defendant's other web pages. Futuredontics claimed that such framing constituted the creation of an infringing derivative work. The defendant moved to dismiss the complaint for failure to state a claim, arguing that its frame should be viewed as merely a "lens" which enabled Internet users to view the information that Futuredontics itself placed on the Internet. The court denied the defendant's motion, ruling that existing authority did not resolve the legal issue, and

⁴⁰¹⁸ "Microsoft Answers Ticketmaster's Charges of Electronic Piracy," *Andrews Computer & Online Industry Litigation Reporter* (July 1, 1997) at 24421.

⁴⁰¹⁹ Futuredontics, Inc. v. Applied Anagramatics, Inc., 45 U.S.P.Q.2d 2005 (C.D. Cal. 1998).

Futuredontics' complaint therefore sufficiently alleged a copyright infringement claim.⁴⁰²⁰ Interestingly, however, the court had previously denied Futuredontics' motion for a preliminary injunction, ruling that Futuredontics had failed to establish a probability of success.⁴⁰²¹

On July 23, 1998, in an unpublished opinion, the Ninth Circuit affirmed the district court's denial of the preliminary injunction.⁴⁰²² The Ninth Circuit found that Futuredontics had presented no evidence whatsoever of tangible, let alone irreparable, harm from the defendant's framed link to its site. In addition, the Ninth Circuit ruled that "Futuredontics' claim, that the AAI framed link 'falsely implies that AAI – not Futuredontics – is responsible for the success of Futuredontics's dental referral service' even if true, is not tied to any tangible loss of business or customer goodwill."⁴⁰²³

5. The Bernstein Case

In Sept. of 1998, a California judge dismissed without comment a copyright infringement lawsuit, Bernstein v. J.C. Penney, Inc.,⁴⁰²⁴ in which the plaintiff, a professional photographer, sought to hold liable several defendants who maintained links on their websites that eventually led to a Swedish university website where two allegedly infringing photographs of actress Elizabeth Taylor owned by the plaintiff were displayed. Specifically, persons visiting J.C. Penney's website could, through a chain of no less than six links, reach the photographs on the Swedish website.⁴⁰²⁵ The plaintiff Bernstein insisted that J.C. Penney deliberately designed its website so that visitors would be able to see the two photographs of Elizabeth Taylor. Bernstein alleged that the defendants had previously licensed one of the photographs, suggesting that the defendants were trying to benefit from the photographs without paying for them.⁴⁰²⁶ The defendants labeled the suit as based on a bizarre and unprecedented theory that, if accepted,

⁴⁰²⁰ Id. at 2010.

⁴⁰²¹ Id. at 2006.

⁴⁰²² Futuredontics, Inc. v. Applied Anagramatics, Inc., 1998 U.S. App. LEXIS 17012 (9th Cir. July 23, 1998).

⁴⁰²³ Id. at *3.

⁴⁰²⁴ 50 U.S.P.Q.2d 1063 (C.D. Cal. 1998).

⁴⁰²⁵ Id. at 1063; "Judge Dismisses Copyright Claims Based on Linking," *Andrews Computer & Online Industry Reporter* (Oct. 6, 1998) at 3, 3. Defendant Arden, manufacturer of a perfume called "Passion" that was endorsed by Taylor, recited the chain of links that a user would need to follow from Penny's site to reach the allegedly infringing photographs: from Penney's main home page to (1) "Elizabeth Taylor's Passion," a part of the Penney's site, to (2) "Biography," a part of the "Passion" site containing information about Taylor's life, to (3) "work on screen," which took the user to (4) an Internet Movie Database Ltd. (IMDB) site, a completely separate site with no connection to Penney's, to (5) "FTP," a link on the IMDB site that took the user to the Swedish site, from where the user could (6) access the infringing photographs. Id.

⁴⁰²⁶ Id.

would destroy the Internet as a means of worldwide communication, and the judge apparently agreed.⁴⁰²⁷

6. The Intellectual Reserve Case

In Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.,⁴⁰²⁸ the plaintiff was the owner of the copyright in a Mormon Church work titled the “Church Handbook of Instructions” (the “Handbook”). After the defendants were ordered to remove copies of the Handbook from their website, the defendants posted a notice on their website stating that the Handbook was online, and posted three links to other website addresses where the Handbook could be found. The plaintiffs sought to hold the defendants liable for inducement of infringement and contributory infringement.

The court ruled that the defendants were not liable for inducement of infringement, because there was no evidence that the defendants had any direct relationship with the other websites on which the Handbook was available, nor that the defendants had induced the operators of those websites to post the Handbook.⁴⁰²⁹

The court concluded, however, that the defendants could be liable for contributory infringement. Turning first to whether there was any direct infringement to which the defendants could be contributing, the court concluded that when visitors to the sites on which the Handbook was posted displayed the Handbook, an infringing copy of the Handbook was made in the users’ RAM.⁴⁰³⁰ The court then concluded that the defendants were contributorily

⁴⁰²⁷ The defendants argued that the plaintiff’s theory of infringement by multiple linking would have a devastating impact on the Internet and argued that the claim should be dismissed for three reasons: “(1) a company whose product is merely displayed on another entity’s website cannot be held liable for any infringement by the author of that website; (2) linking cannot constitute direct infringement because the computer server of the linking website does not copy or otherwise process the content of the linked-to site; and (3) multiple linking cannot constitute contributory infringement because (a) Internet users viewing of the material at issue is not infringing and thus there was no direct infringement in the United States to which Arden could contribute; (b) linking ‘is capable of substantial noninfringing uses’ and thus cannot support a claim for contributory infringement; and (c) the Court cannot infer from the facts alleged that [defendants] knew the photos had been posted to [one of the websites in the chain] and multiple linking does not constitute substantial participation in any infringement where the linking website does not mention the fact that Internet users could, by following the links, finding infringing material on another website.” Bernstein, 50 U.S.P.Q.2d at 1064 (citations omitted). The court dismissed the complaint without leave to amend without articulating any specific reasons therefor. Id.

⁴⁰²⁸ 53 U.S.P.Q.2d 1425 (D. Utah 1999).

⁴⁰²⁹ Id. at 1427.

⁴⁰³⁰ Id. at 1428, citing MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511, 518 (9th Cir. 1993) and Marobie-FL, Inc. v. National Ass’n of Fire Equip. Distrib., 983 F. Supp. 1167, 1179 (N.D. Ill. 1997).

liable for such infringement because they had actively encouraged it,⁴⁰³¹ based on the following facts:

The defendants posted on their website the comment “Church Handbook of Instructions is back online!” and provided three links to websites containing the Handbook.

The defendants posted e-mail suggesting that the lawsuit against the defendants would be affected by people logging into one of the linked websites and downloading the complete Handbook.

In response to an e-mail stating that the sender had unsuccessfully tried to browse a website containing the Handbook, the defendants gave further instruction on how to browse the material.

At least one of the three linked websites encouraged the copying and posting of copies of allegedly infringing material on other websites.⁴⁰³²

Accordingly, the court entered a preliminary injunction enjoining the defendants from, among other things, posting on their website the addresses of other websites that the defendants knew, or had reason to know, contained the material alleged to infringe the plaintiff’s copyright.⁴⁰³³

7. Ticketmaster v. Tickets.com

Ticketmaster Corporation operated the Ticketmaster web site, through which users could purchase tickets to various events such as concerts and ball games. On the Ticketmaster home page there were instructions and a directory to subsequent pages (one per event) containing a short description of the event, date, time, place, and price, and a description of how to order tickets via the Internet, telephone, mail, or in person. The defendant, Tickets.com, operated a somewhat different ticketing service. Although Tickets.com sold some tickets to certain events on its own, it provided information as to where and how tickets that it did not sell could be purchased and a link that would take users to the appropriate ticket seller on line. Where the exclusive ticket broker was Ticketmaster, Tickets.com would deep link directly to the interior web page of Ticketmaster (bypassing the home page) for the particular event in question, where the customer could buy the tickets from Ticketmaster.⁴⁰³⁴

⁴⁰³¹ The court noted that “[l]iability for contributory infringement is imposed when ‘one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another.’” Intellectual Reserve at 1427 (quoting Gershwin Publ’g Corp. v. Columbia Artists Mgt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)).

⁴⁰³² Intellectual Reserve at 1428.

⁴⁰³³ Id. at 1429.

⁴⁰³⁴ Ticketmaster Corp. v. Tickets.com Inc., 54 U.S.P.Q.2d 1344, 1345 (C.D. Cal. 2000).

Ticketmaster alleged that Tickets.com committed copyright infringement by copying its interior web pages in order to extract the basic information on those pages, such as event, place, time, date, and price. (The extracted information was then placed in Tickets.com's format on its own interior web pages.) The court denied a motion by Tickets.com to dismiss the copyright infringement claim, ruling that, although the factual data contained on Ticketmasters' internal pages could not be protected by copyright, the allegation of copying of Ticketmasters' internal web pages in order to extract that factual data was sufficient to state a valid claim for copyright infringement.⁴⁰³⁵ The court went on to state, however, that hyperlinking by itself did not constitute copyright infringement:

[H]yperlinking does not itself involve a violation of the Copyright Act (whatever it may do for other claims) since no copying is involved. The customer is automatically transferred to the particular genuine web page of the original author. There is no deception in what is happening. This is analogous to using a library's card index to get reference to particular items, albeit faster and more efficiently.⁴⁰³⁶

Five months later, the court issued another opinion that denied a motion for a preliminary injunction brought by Ticketmaster. With respect to the copyright claim, the court noted that Ticketmasters' internal web pages were copied only temporarily, for 10-15 seconds, in the course of extracting the factual information from those pages, and the factual information was then presented by Tickets.com to its users in a different format from how that information appeared on Ticketmasters' site.⁴⁰³⁷ The court ruled that the plaintiff was not entitled to a preliminary injunction on copyright grounds because the temporary copying for purposes of extracting the factual information from Ticketmasters' internal web pages was likely to be a fair use. The court analogized to the Ninth Circuit's decision in Sony Computer Entertainment, Inc. v. Connectix Corp.,⁴⁰³⁸ which the district court characterized as holding that copying for reverse engineering to obtain non-protectable information is permitted by the fair use doctrine in certain circumstances.⁴⁰³⁹ The district court observed:

⁴⁰³⁵ Id. at 1345-46. The court granted, however, the defendant's motion to dismiss the plaintiff's breach of contract claim, which was based on the "terms and conditions" for use of the Ticketmasters website. The court apparently found that the terms and conditions were not enforceable because they did not require clicking to "agree" to them and were not immediately visible to users: "[T]he terms and conditions are set forth so that the customer needs to scroll down the home page to find and read them. Many customers instead are likely to proceed to the event page of interest rather than reading the 'small print.' It cannot be said that merely putting the terms and conditions in this fashion necessarily creates a contract with any one using the web site. The motion is granted with leave to amend in case there are facts showing Tickets' knowledge of them plus facts showing implied agreement to them." Id. at 1346.

⁴⁰³⁶ Id. at 1346.

⁴⁰³⁷ Ticketmaster Corp. v. Tickets.com, Inc., 2000 U.S. Dist. LEXIS 12987 at *9-10 (C.D. Cal. Aug. 10, 2000).

⁴⁰³⁸ 203 F.3d 596 (9th Cir. 2000).

⁴⁰³⁹ Tickets.com, 2000 U.S. Dist. LEXIS 12987 at *12.

Reverse engineering to get at unprotected functional elements is not the same process as used here but the analogy seems to apply. The copy is not used competitively. It is destroyed after its limited function is done. It is used only to facilitate obtaining non-protectable data – here the basic factual data. It may not be the only way of obtaining that data (i.e., a thousand scribes with pencil and paper could do the job given time), but it is the most efficient way, not held to be an impediment in *Connectix*.⁴⁰⁴⁰

The court also rejected the plaintiff's argument that the defendant's copying of the URLs of the interior pages of the Ticketmaster's site constituted infringement. "The court doubts that the material is protectable because the URL appears to contain functional and factual elements only and not original material."⁴⁰⁴¹ Accordingly, the court ruled that, because Ticketmaster appeared unlikely to prevail on its copyright infringement claim, a preliminary injunction should not issue.⁴⁰⁴²

After nearly two additional years of litigation, Tickets.com brought a motion for summary judgment on Ticketmaster's copyright claims, which the court granted.⁴⁰⁴³ In granting summary judgment, the court ruled that the spider's temporary copying of Ticketmaster's web pages into RAM in order to extract the factual information about events contained on those pages constituted a fair use. "In temporarily downloading [Ticketmaster's] event pages to its RAM through the use of spiders, [Tickets.com] was not exploiting [Ticketmaster's] creative labors in any way: its spiders gathered copyrightable and non-copyrightable information alike but then immediately discarded the copyrighted material. It is unlikely that the spiders could have been

⁴⁰⁴⁰ *Id.* at *12-13.

⁴⁰⁴¹ *Id.* at *13.

⁴⁰⁴² *Id.*

⁴⁰⁴³ *Ticketmaster Corp. v. Tickets.com, Inc.*, 2003 U.S. Dist. LEXIS 6483 (C.D. Cal. Mar. 7, 2003). Tickets.com also sought summary judgment on Ticketmaster's contract claim, based on a notice placed on the home page of the Ticketmaster site stating that anyone going beyond that point into the interior pages of the web site accepted certain conditions, including that all information obtained from the site was for the personal use of the user and could not be used for commercial purposes. The contract claim had been rejected as a basis for a preliminary injunction in the court's first opinion in 2000, because the notice was placed at the bottom of the home page so that a user without an especially large screen would have to scroll down to read the conditions of use. Subsequently, Ticketmaster moved the notice to a prominent place on the home page with a warning that proceeding further bound the user to the conditions of use. *Id.* at *6-7. In addition, the court noted that Ticketmaster had submitted evidence that Tickets.com was in fact fully familiar with the conditions Ticketmaster claimed to impose on users, including a letter from Ticketmaster to Tickets.com which quoted the conditions, and a reply by Tickets.com stating that it did not accept the conditions. The court denied Tickets.com's motion for summary judgment on the contract theory, noting that there was sufficient evidence to defeat summary judgment on the contract theory if knowledge of the asserted conditions of use was had by Tickets.com. *Id.* at *7-8. The court concluded that "a contract can be formed by proceeding into the interior web pages after knowledge (or, in some cases, presumptive knowledge) of the conditions accepted when doing so." *Id.* at *9.

programmed to take only the factual information from the [Ticketmaster] web pages without initially downloading the entire page.”⁴⁰⁴⁴

The court also reaffirmed its earlier ruling on Ticketmaster’s preliminary injunction motion that the URLs copied by Tickets.com to allow the deep linking were not copyrightable. Ticketmaster contended that, although the URLs were functional, they should be entitled to copyright protection because there were several ways to write the URL and, thus, original authorship was present. The court rejected this argument. “A URL is simply an address, open to the public, like the street address of a building, which, if known, can enable the user to reach the building. There is nothing sufficiently original to make the URL a copyrightable item, especially the way it is used.”⁴⁰⁴⁵

Finally, the court ruled that Tickets.com’s deep linking did not cause an infringing public display of the Ticketmaster event pages. The court distinguished the Ninth Circuit’s holding in Kelly v. Arriba Soft Corp., discussed in Section II.C.2 above, by noting that in Kelly the plaintiff’s images were framed by the defendant’s window and thus were surrounded by the defendant web page’s text and advertising. In the instant case, whether or not framing occurred depended upon the settings on the user’s computer, over which Tickets.com had no control, and framing therefore occurred on some occasions but not on others. However, when users were linked to the Ticketmaster web pages, the user of the Tickets.com site was taken directly to the originating Ticketmaster site, containing all the elements of that particular Ticketmaster event page, and the Ticketmaster event pages were clearly identified as belonging to Ticketmaster. Moreover, the link on the Tickets.com site contained a notice stating “Buy this ticket from another online ticketing company.”⁴⁰⁴⁶ Accordingly, the court granted Tickets.com summary judgment on Ticketmaster’s copyright claims.⁴⁰⁴⁷

8. The MP3Board Case

In this case, several RIAA member companies brought claims for contributory and vicarious copyright infringement against MP3Board for operating a web site, located at www.mp3board.com, which provided Internet users with resources to enable them to locate MP3 files from publicly available Web sites. No music files were located on the MP3Board web

⁴⁰⁴⁴ Id. at *17-18.

⁴⁰⁴⁵ Id. at *20.

⁴⁰⁴⁶ Id. at *21-23.

⁴⁰⁴⁷ Ticketmaster also brought a trespass to chattels claim against Tickets.com based on Tickets.com’s spiders unauthorized entry into the Ticketmaster site. The court granted Tickets.com summary judgment on this claim, ruling that in order to establish a trespass to chattels claim, there must be some evidence of tangible interference with the use or operation of the computer being invaded by the spider. “Since the spider does not cause physical injury to the chattel, there must be some evidence that the use or utility of the computer (or computer network) being ‘spiderized’ is adversely affected by the use of the spider. No such evidence is presented here. This court respectfully disagrees with other district courts’ finding that mere use of a spider to enter a publicly available web site to gather information, without more, is sufficient to fulfill the harm requirement for trespass to chattels.” Id. at *12.

site. Instead, the web site featured an automated search engine that searched for, aggregated and organized links to media files on the Web, and provided a tutorial offering users instruction on how to locate and download such files. The site also featured a message board on which users could post questions or song requests. In response to users' posts, MP3Board personnel personally searched for links to songs and posted the links on the message board, solicited other users to provide the requested works, and obtained and posted passwords to enable users to access certain music files.⁴⁰⁴⁸

The RIAA sent a number of infringement demand letters relating to MP3Board's activities before filing suit. On Oct. 27, 1999, and again on Apr. 18, 2000, the RIAA sent letters to MP3Board's ISP, identifying artists whose works were being infringed – but no specific song titles – and demanding that the ISP remove or disable access to the MP3Board site or MP3Board's links to infringing works. In response to the second letter, MP3Board's ISP disabled Internet access to the MP3Board web site, but service was restored after MP3Board supplied a counter notification to the ISP asserting that it had removed the infringing material identified in the RIAA's notice. On May 25, 2000, the RIAA wrote directly to MP3Board and demanded that MP3Board remove all infringing links, this time naming 21 artists and 22 song titles which were representative of the titles being infringed. The letter also attached printouts of screen shots of MP3Board's web site on which the RIAA identified 662 links which the RIAA believed to lead to infringing material. MP3Board did not dismantle access to any of the identified links in response. Shortly thereafter, the RIAA filed suit and sought summary judgment on its claims of contributory and vicarious copyright infringement.⁴⁰⁴⁹

The court denied the RIAA's motion for summary judgment, finding that numerous issues of material fact remained to be resolved. First, although the structure of the MP3Board site and scale of the operation gave rise to a strong inference that users downloaded files containing copyrighted music, the court found that the record companies had not submitted any direct evidence of infringement to which MP3Board could contribute or be vicariously liable, such as user logs or other technical data showing the downloading of copyrighted and unauthorized files.⁴⁰⁵⁰ The court ruled that, to show the unlawful distribution of a copyrighted work, the plaintiffs needed to show that an unlawful copy was disseminated to the public.⁴⁰⁵¹ This ruling is in contrast to the Frena, Chuckleberry, Webbworld, and Marobie-FL cases, discussed in Section II.D.1 above, which held that the mere making available of unauthorized works for download by members of the public constituted infringement of the distribution right.

With respect to contributory liability, the court found material issues of fact both concerning the knowledge and the material contribution prongs. With respect to the material contribution prong, the court noted that MP3Board styled itself as a "passive" tool. The court

⁴⁰⁴⁸ Arista Records, Inc. v. MP3Board, Inc., 2002 U.S. Dist. LEXIS 16165 at *5-6 (S.D.N.Y. 2002).

⁴⁰⁴⁹ Id. at *7-9.

⁴⁰⁵⁰ Id. at *11-12.

⁴⁰⁵¹ Id. at *13-14.

concluded, however, that there was sufficient evidence from which a factfinder could determine that MP3Board materially contributed to the infringement by virtue of its search engine, the site's solicitation of third parties to post links to sites containing audio files, the posting of a link to a third party named Freedrive where users could store audio files online, the posting of a tutorial on how to locate and download audio files via MP3Board using one of the record companies' copyrighted recordings as an example, and the searching by MP3Board personnel for links to requested songs in response to user requests through the MP3Board message boards.⁴⁰⁵²

Concerning knowledge, the court found material issues of fact with respect to whether MP3Board had constructive knowledge of infringement or whether MP3Board's activities were covered by the Sony doctrine and whether the site was capable of commercially significant noninfringing uses. The record companies pointed to a category of links on the site titled "Legal MP3s" as evidence that MP3Board recognized that the other categories contained MP3s which were not legal. In response, MP3Board noted that a third party MP3 supplier had specifically requested the title "Legal MP3s" to describe the category, which contained exclusively content from that third party. MP3Board also contended that there was no evidence it monitored the posting of links, and stated that it did not investigate the links.⁴⁰⁵³

The court found stronger evidence of actual knowledge of infringement. The court noted that the RIAA letters of Oct. 27, 1999 and Apr. 18, 2000 to MP3Board's ISP, which were forwarded on to MP3Board, were insufficient to constitute notice under DMCA Section 512(d)(3). "By solely listing artists' names, and neglecting to specify any infringing links or even particular songs, the letter(s) did not include 'identification of the reference or link, to material or activity claimed to be infringing.'"⁴⁰⁵⁴ Accordingly, MP3Board's failure to delete any links in response to those letters could not give rise to any liability.⁴⁰⁵⁵ However, the letter of May 25, 2000 complied with DMCA notification requirements because it not only named particular artists along with specified songs, but was accompanied by printouts of screen shots of MP3Board's web site, on which the RIAA highlighted and placed an asterisk next to 662 links which the RIAA believed to infringe upon the record companies' copyrights (although no URL addresses were provided by the RIAA).⁴⁰⁵⁶ Despite the adequacy of notice via the May 25, 2000 letter, the court nevertheless held that issues of material fact existed regarding MP3Board's knowledge of infringing activity.⁴⁰⁵⁷

With respect to vicarious liability, the court similarly found that issues of material fact concerning MP3Board's right and ability to control infringing activity, and whether it had a direct

⁴⁰⁵² Id. at *17-18.

⁴⁰⁵³ Id. at *21-23.

⁴⁰⁵⁴ Id. at *26 (quoting Section 512(d)(3)).

⁴⁰⁵⁵ Id. at *27.

⁴⁰⁵⁶ Id. at *28-29.

⁴⁰⁵⁷ Id. at *30.

financial interest in the activity, precluded summary judgment. It also found material issues of fact concerning whether MP3Board qualified as a “service provider” for purposes of the Section 512(d) safe harbor, thereby at least implicitly recognizing that the Section 512(d) safe harbor could apply to vicarious liability. With respect to the issue of control, the court curiously found issues of material fact, even though it stated, citing the Ninth Circuit’s Napster I decision, that a defendant’s ability to block infringers’ access to a particular environment for any reason constitutes proof of its right and ability to supervise and control the infringing activities. The court further noted as evidence of control that MP3Board could delete links from its database and thus prevent them from being displayed in response to user queries, and that it had in fact removed offending links from the site and banned repeat offenders of its rules from posting any additional links.⁴⁰⁵⁸

With respect to the issue of financial benefit, the court again curiously found issues of material fact, despite the fact that it cited only evidence from which direct financial benefit could be inferred. Specifically, the court, against citing Napster I, noted that infringement which increases a defendant’s user base or otherwise acts as a draw for customers constitutes a direct financial interest. It also cited testimony from MP3Board’s principals that the revenue MP3Board received from banner advertisements on the site was directly tied to the number of users who were exposed to those ads.⁴⁰⁵⁹ In view of the material issues of fact cited by the court, it denied the plaintiffs’ motion for summary judgment.⁴⁰⁶⁰

9. Kelly v. Arriba Soft

One of the most important linking cases is that of Kelly v. Arriba Soft Corp.⁴⁰⁶¹ That case and its significance are discussed in detail in Section II.C.2 above.

10. Batesville Services, Inc. v. Funeral Depot, Inc.

In Batesville Services, Inc. v. Funeral Depot, Inc.,⁴⁰⁶² the plaintiff Batesville sold caskets and was the owner of the copyrights in a number of advertising photographs used to market its caskets. The defendant, although not an authorized dealer of Batesville, operated a web site that sold caskets, including Batesville caskets. The defendant displayed some of Batesville’s casket photographs on its web site. In response to a cease and desist letter, the defendant removed the photographs from its web site, but approached the Veterans Society, an authorized

⁴⁰⁵⁸ Id. at *33-34.

⁴⁰⁵⁹ Id. at *35-36.

⁴⁰⁶⁰ The court denied a counter-motion for summary judgment filed by MP3Board that its activities of identifying links where information could be found were protected by the First Amendment. The court cited authority from the Second Circuit that the fair use doctrine encompasses all claims under the First Amendment in the copyright field, and noted that MP3Board had not asserted that its activities constituted fair use, nor could it succeed on such an assertion under the applicable factors of the fair use doctrine. Id. at *37-40.

⁴⁰⁶¹ No. 00-55521 (9th Cir. Feb. 6, 2002).

⁴⁰⁶² 2004 Copyr. L. Dec. ¶ 28,901 (S.D. Ind. 2004).

Batesville dealer, and reached an agreement that the defendant would pay the expenses of modifying the Veterans Society web site so that digitized versions of images of Batesville caskets would be displayed on the site. The defendant then modified its own web site so that small, low resolution thumbnail images of Batesville caskets were linked to the appropriate casket pages on the Veterans Society website. When a shopper on the defendant's site clicked on a thumbnail image, the shopper was linked to a much larger image on a casket page on the Veterans Society web site, which in turn displayed the defendant's phone number. The casket web pages on the Veterans Society site also had a link labeled "Back to Main Gallery" that would return the viewer to the defendant's web site.⁴⁰⁶³

The plaintiff contended that both the previous and the modified arrangements violated their copyrights in the photographs in question. The defendant argued, among other things, that the Veterans Society, as an authorized Batesville dealer, had an implied license to display the photographs, and that in any event the use of links on the Internet could never amount to copyright infringement. Both sides moved for summary judgment.⁴⁰⁶⁴

With respect to the implied license argument, the court noted that Batesville had supplied the photographs to the Veterans Society as an authorized dealer, and that like any other Batesville dealer, the Veterans Society was authorized to use those photographs for at least some purposes. Batesville argued, however, that the Veterans Society had exceeded the scope of its implied license by posting the photographs on its web site to promote a business other than its own. The court rejected this argument, noting that there was no evidence that Batesville had even asked the Veterans Society to change its arrangements or had ever communicated to the Veterans Society its internal policy that its photographs were to be used to promote only the authorized dealer's business to whom the photographs were supplied. Batesville could have revoked at any time the implied license to the Veterans Society or insisted that it revise its web site in a way that satisfied Batesville, but had not done so. Accordingly, the factual record could lead a reasonable jury to find that the Veterans Society's implied license allowed the disputed use of the images in question, and the court ruled that neither Batesville nor the defendant was entitled to summary judgment on the implied license defense.⁴⁰⁶⁵

Turning to the defendant's linking defense, the court rejected the defendant's argument, based on the Ticketmaster Corp. v. Tickets case and the Bernstein case, discussed respectively in Sections III.D.7 and III.D.5 above, that links can never amount to a copyright violation. The court noted that those two cases suggest that the host of a web site who establishes a link to another site that may be interesting to the host's web site visitors does not undertake any general duty to police whether the linked sites contain any material infringing the copyrights of others. Those

⁴⁰⁶³ Id. at pp. 37,694-95.

⁴⁰⁶⁴ Id. at 37,695.

⁴⁰⁶⁵ Id. at 37,697-98. The court also rejected the defendant's argument that its use of the Batesville photographs was a fair use. Id. at 37,698-701.

two cases, however, did not support a sweeping per se rule that links can never give rise to infringement.⁴⁰⁶⁶

The court cited the Intellectual Reserve case, discussed in Section III.D.6 above, for the proposition that, in extreme cases, even encouraging browsing of infringing web sites can violate the copyright laws.⁴⁰⁶⁷ “From that conclusion, it is easy to allow room for liability for defendants who deliberately encourage use of infringing web sites by establishing links to those sites. This is not a case where Funeral Depot merely found some useful material elsewhere on the internet and encouraged its shoppers to link to those sites. Instead, Funeral Depot actively secured control of the contents of the Veterans Society website and modified the website to use it for its own purposes.”⁴⁰⁶⁸

The court noted that the “casket gallery” on the Veterans Society web site did not exist until the defendant created those web pages, that it had designed and paid for them, it still controlled changes to them, and they displayed the defendant’s phone number. The defendant’s control of the web pages was so complete that the owner of the Veterans Society was not aware of any changes to the casket portion of its web site.⁴⁰⁶⁹ “These facts are unusual enough to take this case out of the general principle that linking does not amount to copying. These facts indicate a sufficient involvement by Funeral Depot that could allow a reasonable jury to hold Funeral Depot liable for copyright infringement or contributory infringement, if infringement it is. The possibility of copyright infringement liability on these unusual facts showing such extensive involvement in the allegedly infringing display should not pose any broad threat to the use of hyperlinks on the internet.”⁴⁰⁷⁰

11. Live Nation Sports v. Davis

The facts of Live Nation Motor Sports, Inc. v. Davis,⁴⁰⁷¹ are discussed in Section II.B.3 above. The court granted a preliminary injunction enjoining the defendant from providing Internet links to the plaintiff’s webcasts of its motorcycle racing events or otherwise displaying or performing the plaintiff’s webcasts.⁴⁰⁷² With almost no analysis, the court ruled that the plaintiff had a likelihood of success on its copyright claim because “the unauthorized ‘link’ to the live webcasts that [the defendant] provides on his website would likely qualify as a copied display or performance of [the plaintiff’s] copyrightable material.”⁴⁰⁷³ The court found a threat of irreparable harm to the plaintiff because the defendant’s links would cause the plaintiff to lose

⁴⁰⁶⁶ Id. at 37,701.

⁴⁰⁶⁷ Id. at 37,701-02.

⁴⁰⁶⁸ Id. at 37,702.

⁴⁰⁶⁹ Id.

⁴⁰⁷⁰ Id.

⁴⁰⁷¹ 2006 U.S. Dist. LEXIS 89552 (N.D. Tex. Dec. 11, 2006).

⁴⁰⁷² Id. at *18.

⁴⁰⁷³ Id. at *12.

its ability to sell sponsorships or advertisements on the basis that its website was the exclusive source of the webcasts.⁴⁰⁷⁴ Although the unclear facts of this case make its reach uncertain, it could potentially imply that any unauthorized link that causes material available on another site to be streamed through an unauthorized site could constitute an infringing public display or performance.

12. Perfect 10 v. Google (aka Perfect 10 v. Amazon)

The case of Perfect 10 v. Google involved some important rulings in the context of framing of content taken from third party sites. That case is discussed extensively in Section II.C.4 above.

13. Pearson Education v. Ishayev

In Pearson Education, Inc. v. Ishayev,⁴⁰⁷⁵ the plaintiffs were the publisher of both textbooks and solutions manuals for those textbooks. The plaintiffs sued the defendants for copyright infringement for the unauthorized sale and distribution of the solutions manuals, based both on emailing ZIP files containing digital copies of the manuals and sending hyperlinks referencing a web site, filesonic.com, from which the manuals could be purchased and downloaded. The court ruled that, although the former activity constituted direct infringement, the latter did not:⁴⁰⁷⁶

As a matter of law, sending an email containing a hyperlink to a site facilitating the sale of a copyrighted work does not itself constitute copyright infringement. A hyperlink (or HTML instructions directing an internet user to a particular website) is the digital equivalent of giving the recipient driving directions to another website on the Internet. A hyperlink does not itself contain any substantive content; in that important sense, a hyperlink differs from a zip file. Because hyperlinks do not themselves contain the copyrighted or protected derivative works, forwarding them does not infringe on any of a copyright owner's five exclusive rights under § 106.⁴⁰⁷⁷

⁴⁰⁷⁴ Id. at *15.

⁴⁰⁷⁵ 963 F. Supp. 2d 239 (S.D.N.Y. 2013).

⁴⁰⁷⁶ Id. at 242, 249-50 & n.9.

⁴⁰⁷⁷ Id. at 250-51. In support of its conclusion, the court cited the Perfect 10 v. Amazon and Arista Records v. MP3Board cases discussed in subsections III.D.8 and III.D.12 above, as well as MyPlayCity, Inc. v. Conduit Ltd., 2012 U.S. Dist. LEXIS 47313 at *12 (S.D.N.Y. Mar. 30, 2012) ("Because the actual transfer of a file between computers must occur, merely providing a 'link' to a site containing copyrighted material does not constitute direct infringement of a holder's distribution right.") The court noted that the defendant who had sent the hyperlinks attested that he was not responsible for uploading the infringing material to filesonic.com, and that the plaintiffs' evidence that he reproduced or participated in the reproduction of the plaintiffs' solutions manuals before furnishing the emails containing the hyperlinks was not conclusive. Id. at 251-52.

E. Streaming and Downloading

“Streaming” is the digital transmission of a work, usually a musical work, over a network that results in an immediate playing of the work at the recipient’s end, without storage of a permanent copy at the recipient’s end. If a permanent copy of a work is stored at the recipient’s end as a result of a transmission, the act of transmission is usually referred to as “downloading” and the resultant copy is referred to as a “download.” A “limited download” refers to a download that can be played only for a limited period of time or a limited number of plays.

Streaming potentially implicates at least two rights of the copyright holder in both the sound recording being transmitted and the musical work embodied in the sound recording – the right of public performance and the right of reproduction. The right of public performance is potentially implicated because Section 101 of the copyright statute defines the public performance of a work to include the following: “to transmit or otherwise communicate a performance ... of the work ... to the public, by means of any device or process, whether the members of the public capable of receiving the performance ... receive it in the same place or in separate places and at the same time or at different times.”⁴⁰⁷⁸ The right of reproduction is potentially implicated because interim whole or partial copies of the work are made in various RAM memories in the course of transmission of the work through the Internet.⁴⁰⁷⁹ In addition, copies of the works available for streaming generally must be stored on one or more servers operated by the streaming vendor.

Significant legal disputes have arisen over the application of the rights of public performance and reproduction, as well as the compulsory statutory licenses afforded by the copyright statute, to streaming and limited downloads. The nature of these disputes, and the cases decided to date with respect to them, are discussed below.

1. The Digital Performance Right – The Section 114(d)(1) Exemption and Streaming by FCC-Licensed Broadcasters

Section 106 (4) of the copyright statute grants the owner of copyright in a work the exclusive right to perform the work publicly. The right does not apply, however, to sound recordings,⁴⁰⁸⁰ except with respect to certain public performances by digital transmission. In particular, the Digital Performance Right in Sound Recordings Act of 1995 (DPRA)⁴⁰⁸¹ created as

⁴⁰⁷⁸ 17 U.S.C. § 101.

⁴⁰⁷⁹ See the analysis in Sections I.A.1 & I.A.2 above.

⁴⁰⁸⁰ 17 U.S.C. § 114(a).

⁴⁰⁸¹ Pub. L. No. 104-39, 109 Stat. 336 (codified at 17 U.S.C. §§ 106, 114, 115).

of February 1, 1996 a limited right to perform a sound recording by means of a “digital audio transmission.”⁴⁰⁸²

Certain digital transmissions of performances are exempt from this right under Section 114(d)(1). Specifically, the performance of a sound recording publicly by means of a digital audio transmission (i) as part of a “nonsubscription broadcast transmission,”⁴⁰⁸³ (ii) as part of a retransmission of a nonsubscription broadcast transmission (subject to certain limitations in the case of a retransmission of a radio station’s broadcast transmission),⁴⁰⁸⁴ or (iii) as part of certain other narrowly defined incidental transmissions or transmissions within or to a business establishment for use in the ordinary course,⁴⁰⁸⁵ is exempt from the digital performance right, provided in each case that it is not “part of an interactive service.” The copyright statute defines an “interactive service” as a service “that enables a member of the public to receive a transmission of a program specially created for the recipient, or on request, a transmission of a particular sound recording, whether or not as part of a program, which is selected by or on behalf of the recipient.”⁴⁰⁸⁶ Nonexempt digital audio transmissions that are not part of an “interactive service” are subject to a statutory license as provided in Section 114(d)(2) of the copyright statute, as discussed further in subsection 2 below. Those wishing to engage in digital audio transmissions as part of an interactive service must negotiate individual licenses with the relevant copyright holders.

In the late 1990’s, a controversy arose over whether FCC-licensed broadcasters, which are exempt from paying royalties to sound recording copyright holders for traditional radio broadcasting of those recordings, should remain exempt when streaming the same broadcast over the Internet. The broadcasters argued such streaming should be classified as an exempt “nonsubscription broadcast transmission” under Section 114(d)(1)(A) of the copyright statute. On Dec. 11, 2000, the Copyright Office issued a final rule determining that AM/FM broadcast signals transmitted simultaneously over a digital communications network such as the Internet

⁴⁰⁸² See 17 U.S.C. § 106(6). Section 114(j)(5) of the copyright statute defines a “digital audio transmission” to mean “a digital transmission as defined in section 101, that embodies the transmission of a sound recording. This term does not include the transmission of any audiovisual work.” Section 101 defines “digital transmission” as “a transmission in whole or in part in a digital or other non-analog format.”

⁴⁰⁸³ 17 U.S.C. § 114(d)(1)(A). A “broadcast” transmission is “a transmission made by a terrestrial broadcast station licensed as such by the Federal Communications Commission.” *Id.* § 114(j)(3). A “nonsubscription” transmission is “any transmission that is not a subscription transmission.” *Id.* § 114(j)(9). A “subscription” transmission is “a transmission that is controlled and limited to particular recipients, and for which consideration is required to be paid or otherwise given by or on behalf of the recipient to receive the transmission or a package of transmissions including the transmission.” *Id.* § 114(j)(14).

⁴⁰⁸⁴ *Id.* § 114(d)(1)(B).

⁴⁰⁸⁵ *Id.* § 114 (d)(1)(C).

⁴⁰⁸⁶ *Id.* § 114(j)(7).

were not exempt under Section 114(d)(1)(A), and thus were subject to the digital performance right of the DPRA.⁴⁰⁸⁷

In its ruling, the Copyright Office determined that the exemption for “broadcast transmission[s]” was limited to over-the-air transmissions by FCC-licensed broadcasters and thus did not cover streaming.⁴⁰⁸⁸ The Copyright Office also amended its regulatory definition of a “Service” for purposes of the Section 114 statutory license to clarify that transmissions of a broadcast signal over a digital communications network such as the Internet are not exempt from copyright liability under Section 114(d)(1)(A) of the Copyright Act. The broadcasters challenged the Copyright Office’s ruling in federal court.

In Bonneville Int’l Corp. v. Peters,⁴⁰⁸⁹ the Third Circuit affirmed a district court’s ruling upholding the Copyright Office’s ruling. The Third Circuit noted that, for AM/FM webcasting to be exempt under Section 114(d)(1)(A) from the digital audio transmission performance copyright, it must be 1) noninteractive, 2) nonsubscription and 3) broadcast. Because the parties agreed that AM/FM webcasting was not part of an interactive service and was a nonsubscription transmission, the issue was whether AM/FM webcasting is a “broadcast transmission.”⁴⁰⁹⁰

The court concluded from the statutory language and the legislative history that AM/FM webcasting is not a broadcast transmission. With respect to the statutory language, Section 114(j)(3) defines a broadcast transmission as “a transmission made by a terrestrial broadcast station licensed as such by the Federal Communications Commission.” The court gave “terrestrial” its “natural and logical meaning of earthbound.”⁴⁰⁹¹ The parties disputed, however, whether a “broadcast station” should be read to refer to the broadcaster as a business entity that operates broadcasting facilities, or to the broadcasting facilities themselves (and by extension the mode of transmission). The court adopted the latter interpretation, noting that the former interpretation would lead to anomalous consequences. One such consequence would be that any entity that operated at least one FCC-licensed radio station would have carte blanche to digitally perform recordings via any conceivable transmission medium (in a noninteractive, nonsubscription manner) without limitation or copyright liability.⁴⁰⁹²

Another anomalous consequence would be that the meaning of the modifier “terrestrial” would become absurd. Specifically, under the interpretation in question, a terrestrial broadcast station would mean a business entity that is earthbound, in contrast, presumably, to one that is space-borne. The court noted that such an interpretation made no sense given that no space-borne business entities exist. On the other hand, an interpretation limited to earthbound

⁴⁰⁸⁷ 65 Fed. Reg. 77292 (Dec. 11, 2000).

⁴⁰⁸⁸ Id. at 77301.

⁴⁰⁸⁹ 68 U.S.P.Q.2d 1545 (3d Cir. 2003).

⁴⁰⁹⁰ Id. at 1549.

⁴⁰⁹¹ Id. at 1550.

⁴⁰⁹² Id.

broadcasting *facilities*, as opposed to broadcasting done through satellites, would be entirely plausible.⁴⁰⁹³ Accordingly, the court concluded that a

“broadcast station licensed as such by the [FCC],” as the term is used in Section 114(j)(3), refers to the physical radio station facility that broadcasts radio signals over the air, and not to the business entity that operates the radio station. A “broadcast transmission” under § 114(d)(1)(A) would therefore be a radio transmission by a radio station facility operated subject to an FCC license and would not include a webcast. AM/FM webcasting does not meet the definition of a “nonsubscription broadcast transmission” and does not, therefore, qualify under § 114(d)(1)(A) for an exemption from the digital audio transmission performance copyright of § 106(6).⁴⁰⁹⁴

The court noted that the legislative history was consistent with its interpretation. In the 1995 Senate Report, accompanying the legislation that first established a digital performance right for sound recordings, Congress stated that the “classic example of [an exempt transmission under section 114(d)(1)(A)] is a transmission to the general public by a free *over-the-air* broadcast station, such as a traditional radio or television station, and the Committee intends that such transmissions be exempt regardless of whether they are in a digital or nondigital format, in whole or in part.”⁴⁰⁹⁵ Thus, the court found it clear that the original 1995 exemption for broadcast transmissions was limited to over-the-air transmissions, and Congress did not contemplate protecting AM/FM webcasting, which did not exist at the time. Because the DMCA amendments in 1998 to the broadcast transmission exemptions were silent on AM/FM webcasting, the court found no affirmative grounds to believe that Congress intended to expand the protections contemplated by the original 1995 legislation.⁴⁰⁹⁶

Accordingly, the Third Circuit concluded that Section 114(d)(1)(A)’s nonsubscription broadcast transmission exemption implicates only over-the-air radio broadcast transmissions, and does not cover the Internet streaming of AM/FM broadcast signals.⁴⁰⁹⁷

As discussed in detail in Section III.E.2(a) below, in May of 2003, the Digital Media Association, the American Federation of Television and Radio Artists, the American Federation of Musicians of the United States and Canada, and the RIAA agreed on a proposal for royalty rates to be paid for Internet streaming of AM/FM broadcasts for the period from 1998 through Dec. 31, 2004, and submitted the proposal to the Copyright Office for possible adoption without a CARP. On May 20, 2003, the Copyright Office published the proposal for comment.⁴⁰⁹⁸

⁴⁰⁹³ Id.

⁴⁰⁹⁴ Id. at 1552.

⁴⁰⁹⁵ S. Rep. No. 104-128, at 19 (1995).

⁴⁰⁹⁶ Id. at 1555.

⁴⁰⁹⁷ Id.

⁴⁰⁹⁸ 68 Fed. Reg. 27506 (May 20, 2003).

With respect to the related issue of royalties to owners of the copyrights in underlying musical works that are streamed online, in Nov. 2001, a federal district court in New York approved an interim agreement reached between radio stations and music-licensing agency Broadcast Music Inc. (BMI). Under that agreement, radio stations agreed to pay 1.065% of revenues generated by online music streaming, the same rate that radio stations pay for rights to broadcast the musical compositions over the airwaves.⁴⁰⁹⁹

Similarly, in Oct. 2004, a federal district court in New York approved a license agreement negotiated between the American Society of Composers, Authors and Publishers (ASCAP) and the Radio Music License Committee (RMLC), representing most of the nearly 12,000 U.S. commercial radio stations, for rights to perform ASCAP music over the air and via simultaneous streaming. The agreement governed the period Jan. 1, 2001 through Dec. 31, 2009.⁴¹⁰⁰

2. The Digital Performance Right – Statutory Licenses Under Section 114 for Certain Nonsubscription and Subscription Services

Section 114 of the copyright statute provides statutory licenses for the performance of sound recordings publicly by both nonsubscription and subscription digital services, again provided in each case that such transmissions are “not part of an interactive service.”⁴¹⁰¹ Under Section 114(d)(2), the statutory licenses cover transmissions by the following means:⁴¹⁰²

Subscription Digital Audio Transmissions: by means of subscription digital audio transmissions that are not exempt under Section 114(d)(1). A “subscription” transmission is “a transmission that is controlled and limited to particular recipients, and for which consideration is required to be paid or otherwise given by or on behalf of the recipient to receive the transmission or a package of transmissions including the transmission.”⁴¹⁰³

All nonexempt digital subscription transmission services are eligible for the statutory license, provided that they are non-interactive and comply with the terms of the license.

⁴⁰⁹⁹ Kevin Featherly, “Judge OKs Interim Online-Radio Music Royalty Rate” (Nov. 28, 2001), available as of Feb. 2, 2002 at www.newsbytes.com/news/01/172509.html.

⁴¹⁰⁰ “Music Publishers Sign Deal on Web Radio” (Oct. 18, 2004), available as of Oct. 19, 2004 at www.washingtonpost.com/wp-dyn/articles/A41418-2004Oct.18.html. The court’s order approving the license agreement was available as of May 1, 2005 at www.ascap.com/licensing/radio/ORDER.pdf. The license sets forth the total amount of industry-wide fees that will be collected by ASCAP during each of the applicable years of the agreement, and allocates each local radio station’s share of the annual license payment in accordance with a license fee allocation formula set forth in Exhibit B to the license. A copy of the license was available as of May 1, 2005 at www.ascap.com/licensing/radio/RMLC_License.pdf (main body of license) and www.ascap.com/licensing/radio/FeeMethodology.pdf (allocation formula).

⁴¹⁰¹ 17 U.S.C. § 114(d)(2)(A)(i).

⁴¹⁰² The statutory license was expanded by the Digital Millennium Copyright Act of 1998 (DMCA), Pub. L. No. 105-304, to expressly cover non-exempt eligible non-subscription transmissions and non-exempt transmissions made by preexisting satellite digital audio radio services. See 17 U.S.C. § 114(f).

⁴¹⁰³ 17 U.S.C. § 114(j)(14).

Although the statutory provisions are quite complex, Section 114 generally requires that the service not violate the “sound recording performance complement,”⁴¹⁰⁴ not publish in advance a schedule of the programming to be performed, not cause any receiving device to switch from one program channel to another, include in each transmission certain identifying information encoded in each sound recording, pay the royalty fees, and comply with the associated terms and with any recordkeeping requirements promulgated by the Copyright Office.⁴¹⁰⁵

The statute distinguishes between two types of subscription digital audio transmissions: (1) a “preexisting subscription service,” which is a non-interactive subscription service performing audio-only digital audio transmissions that was in existence and was making such transmissions to the public for a fee on or before July 31, 1998;⁴¹⁰⁶ and (2) a “new subscription service,” which is a non-interactive subscription service performing digital audio transmissions and that is not a preexisting subscription service or a “preexisting satellite digital audio radio service” (defined in the third bullet below).⁴¹⁰⁷

Eligible Nonsubscription Transmissions (Webcasting): by means of an “eligible nonsubscription transmission,” which is defined as “a noninteractive nonsubscription digital audio transmission not exempt under subsection (d)(1) that is made as part of a service that provides audio programming consisting, in whole or in part, of performances of sound recordings, including retransmissions of broadcast transmissions, if the primary purpose of the service is to provide to the public such audio or other entertainment programming, and the primary purpose of the service is not to sell, advertise, or promote particular products or services other than sound recordings, live concerts, or other music-related events.”⁴¹⁰⁸ The

⁴¹⁰⁴ Section 114(j)(13) provides: “The ‘sound recording performance complement’ is the transmission during any 3-hour period, on a particular channel used by a transmitting entity, of no more than-

(A) 3 different selections of sound recordings from any one phonorecord lawfully distributed for public performance or sale in the United States, if no more than 2 such selections are transmitted consecutively; or

(B) 4 different selections of sound recordings-

(i) by the same featured recording artist; or

(ii) from any set or compilation of phonorecords lawfully distributed together as a unit for public performance or sale in the United States,

if no more than three such selections are transmitted consecutively:

Provided, That the transmission of selections in excess of the numerical limits provided for in clauses (A) and (B) from multiple phonorecords shall nonetheless qualify as a sound recording performance complement if the programming of the multiple phonorecords was not willfully intended to avoid the numerical limitations prescribed in such clauses.”

⁴¹⁰⁵ 17 U.S.C. §§ 114(d)(2)(A)-(C) & 114(f)(2)-(4).

⁴¹⁰⁶ *Id.* § 114(j)(11).

⁴¹⁰⁷ *Id.* § 114(j)(8).

⁴¹⁰⁸ *Id.* § 114(j)(6).

conditions for the statutory license for eligible nonsubscription transmissions are very similar to those of nonexempt digital subscription transmissions noted above.

Preexisting Satellite Digital Audio Radio Services: by means of a “preexisting satellite digital audio radio service” (not exempt under Section 114(d)(1)), which is defined as “a subscription satellite digital audio radio service provided pursuant to a satellite digital audio radio service license issued by the Federal Communications Commission on or before July 31, 1998, and any renewal of such license to the extent of the scope of the original license, and may include a limited number of sample channels representative of the subscription service that are made available on a nonsubscription basis in order to promote the subscription service.”⁴¹⁰⁹ To be eligible for the statutory license, the service must not exceed the sound recording performance complement and must not publish in advance a schedule of the programming to be performed.⁴¹¹⁰

Pursuant to its statutory authority, the Copyright Office conducted a number of Copyright Arbitration Royalty Panel (CARP) proceedings⁴¹¹¹ to establish the royalty rates to be paid for the statutory license. For example, on May 8, 1998, the Librarian of Congress issued an initial determination of rates and terms for the statutory license to be paid by nonexempt subscription digital transmission services, imposing a royalty rate of 6.5% of gross revenues from U.S. residential subscribers.⁴¹¹²

The Copyright Office subsequently initiated separate CARP proceedings to set rates and terms for transmissions made by “eligible nonsubscription services” and those transmissions made by “pre-existing satellite digital audio radio services.”⁴¹¹³ The latter proceeding was also to establish rates and terms for transmissions made during the period Jan. 1, 2001, to Dec. 31, 2002, by “preexisting subscription services” (i.e., the three subscription services in existence prior to the passage of the DMCA, as discussed in the next subsection). Neither proceeding considered rates and terms for transmissions made by “new subscription services.” The manner

⁴¹⁰⁹ Id. § 114(j)(10).

⁴¹¹⁰ Id. § 114(d)(2)(B).

⁴¹¹¹ The Copyright Royalty Tribunal Reform Act of 1993, Pub. L 103-198, 107 Stat. 2304, eliminated the Copyright Royalty Tribunal (CRT) and replaced it with a system of ad hoc Copyright Arbitration Royalty Panels (CARPs) administered by the Librarian of Congress and the Copyright Office. The CARPs adjust royalty rates and distribute royalties collected under the various compulsory licenses and statutory obligations of the copyright statute.

⁴¹¹² 63 Fed. Reg. 25394 (May 8, 1998). The determination was appealed by the RIAA. The D.C. Circuit affirmed the rates, although it remanded the matter of certain payment terms to the Librarian for further proceedings. Recording Industry Ass'n of Am. v. Librarian of Congress, 176 F.3d 528 (D.C. Cir. 1999).

⁴¹¹³ 66 Fed. Reg. 1700 (Jan. 9, 2001). A “pre-existing satellite digital audio radio service” is “a subscription satellite digital audio radio service provided pursuant to a satellite digital audio radio service license issued by the Federal Communications Commission on or before July 31, 1998, and any renewal of such license to the extent of the scope of the original license, and may include a limited number of sample channels representative of the subscription service that are made available on a nonsubscription basis in order to promote the subscription service.” 17 U.S.C. § 114(j)(10).

in which rates have subsequently been set for the various categories of services are enumerated in the following subsections.

(a) Preexisting Subscription Services

In early 2003, three preexisting subscription services (Music Choice, DMX Music Inc., and Muzak LLC) reached agreement with the RIAA, American Federation of Television and Radio Artists, and American Federation of Musicians of the United States and Canada on what the terms and rates should be for the use of sound recordings by the preexisting subscription services under the Section 114 statutory license. On Jan. 30, 2003, the Copyright Office published the proposed rates and terms for comment on their possible adoption without the convening of a CARP. The proposal covered rates and terms for the period Jan. 1, 2002 through Dec. 31, 2007. SoundExchange would be the agent designated to receive the royalty payments.⁴¹¹⁴ On July 3, 2003, having received no objections, the Copyright Office adopted the proposed rates and terms as final. Licensees were required to pay 7% of monthly gross revenues from residential services in the United States for the period Jan. 1, 2002 through Dec. 31, 2003, and 7.25 % for Jan. 1, 2004 through Dec. 31, 2007. In addition, an advance payment of \$100,000 was required each year, due by Jan. 20 of each year.⁴¹¹⁵

On Nov. 30, 2004, the Copyright Royalty and Distribution Reform Act of 2004 (“CRDRA”)⁴¹¹⁶ was enacted, with an effective date of May 31, 2005. That Act eliminated the CARP system and replaced it with a Copyright Royalty Board (CRB) comprised of three permanent Copyright Royalty Judges (CRJs).

On Jan. 9, 2006, the CRB announced commencement of a proceeding to determine rates and terms of royalty payments under Sections 114 and 112 for preexisting subscription services and preexisting satellite digital audio radio services (“SDARS”).⁴¹¹⁷ SoundExchange, Music Choice, Muzak, XM, Sirius, Royalty Logic Inc. and THP Capstar Acquisition dba DMX Music, all filed petitions in response. DMX and Sirius asserted that they qualified as preexisting subscription services and were thus eligible for the earlier, below-market rates established by the CARP in May 1998 and revised in July 2003. SoundExchange challenged this assertion, arguing that they did not qualify as a preexisting service under Section 114(j)(11) because neither had provided digital audio transmissions on or before July 31, 1998. On Aug. 21, 2006, the CRB referred this question to the Register of Copyrights for a ruling.⁴¹¹⁸

⁴¹¹⁴ 68 Fed. Reg. 4744 (Jan. 31, 2003).

⁴¹¹⁵ 68 Fed. Reg. 39837 (July 3, 2003).

⁴¹¹⁶ Pub. L. No. 108-419, 118 Stat. 2341 (2004).

⁴¹¹⁷ 71 Fed. Reg. 1455 (Jan. 9, 2006).

⁴¹¹⁸ “Copyright Royalty Board Sets New Rates for Satellite Radio Providers XM and Sirius,” *BNA’s Patent, Trademark & Copyright Journal* (Dec. 14, 2007) at 160.

In November of 2006, in response to the CRB's request, the Copyright Office published in the Federal Register a memorandum opinion concluding that

eligibility for a preexisting subscription service license is limited to subscription services that satisfy the definition of 17 U.S.C. § 114(j)(11), which includes being in operation on July 31, 1998 and continuously operating since that time. In 1998, Congress identified those entities which satisfied the definition and were eligible at that time as being DMX, Music Choice and the DISH Network. Therefore, today, those same services are the only ones that may qualify as being preexisting subscription services, since they are the only ones which can satisfy the requirement of being in operation as of July 31, 1998. Moreover, for purposes of participating in a rate setting proceeding, the term 'preexisting subscription service' is best interpreted as meaning the business entity which operates under the statutory license. A determination of whether DMX is the same service that was identified by the legislative history in 1998 and has operated continuously since that time requires a factual analysis that is beyond the scope of the Register's authority for questions presented under 17 U.S.C. § 802(f)(1)(B).⁴¹¹⁹

Over the next year, various parties either entered into independent settlement arrangements with SoundExchange, were dismissed by the CRB, or withdrew from the proceedings, leaving only Sirius and XM to proceed as SDARS.⁴¹²⁰ In June 2007, SoundExchange and Music Choice entered into an agreement that was submitted to the royalty judges pursuant to 17 U.S.C. § 801(b)(7)(A). On Oct. 31, 2008, the CRB published a Notice of Proposed Rulemaking requesting comment on the proposed rates and terms submitted to the CRB. Having received no objections from a party that would be bound by the proposed rates and terms, the CRB adopted them in its final regulations on Dec. 19, 2007, effective Jan. 1, 2008.⁴¹²¹ The rates stipulated that from 2008 through 2011, the royalty fees would be 7.25% of the licensee's monthly gross revenues resulting from residential services in the United States, and for 2012 the fee would be 7.25% of monthly gross revenues. These rates also include a minimum, non-refundable, annual fee of \$100,000, credited against royalties due in that year.⁴¹²² The CRB ruled that these rates were inclusive of the Section 112 ephemeral license, but declined to ascribe any particular percentage of the Section 114 royalty as representative of the value of the Section 112 license.⁴¹²³

On Jan. 10, 2008, the CRB issued its decision setting the statutory royalty rate that XM and Sirius must pay to artists and record labels through 2012 as follows: 6.0% for 2007 and

⁴¹¹⁹ 71 Fed. Reg. 64639, 64640 (Nov. 3, 2006).

⁴¹²⁰ "Copyright Royalty Board Sets New Rates for Satellite Radio Providers XM and Sirius," *BNA's Patent, Trademark & Copyright Journal* (Dec. 14, 2007) at 160-61.

⁴¹²¹ 72 Fed. Reg. 71795 (Dec. 19, 2007); "Fees, Terms Set for Transmission Of Sound Recordings by Preexisting Services," *BNA's Patent, Trademark & Copyright Journal* (Jan. 04, 2008) at 222.

⁴¹²² 72 Fed. Reg. 71795, 71796 (Dec. 19, 2007).

⁴¹²³ Id.

2008; 6.5% for 2009; 7.0% for 2010; 7.5% for 2011; and 8.0% for 2012. The CRB ruled that these rates were inclusive of the Section 112 ephemeral license, but again declined to ascribe any particular percentage of the Section 114 royalty as representative of the value of the Section 112 license.⁴¹²⁴

These decisions were cast in doubt, however, when the Register of Copyrights issued a determination on Feb. 19, 2008 stating that the CRB had committed clear legal error by failing to set separate values for the Section 112 and Section 114 licenses, and failing to include a minimum fee for the Section 112 license. The Register found the failure to set separate values to be problematic because the beneficiaries of each license may not be identical, as the Section 112 statutory license applies to reproductions and the Section 114 statutory license applies to public performances.⁴¹²⁵

The impact of the Register's determination was initially unclear. Although Section 802(f)(1)(D) allows the Register to issue a decision correcting legal errors made by the CRB after a final determination has issued, the CRB may revise final determinations only to correct "technical or clerical errors," or to modify the "terms but not the rates... in response to unforeseen circumstances that would frustrate the proper implementation of such determination."⁴¹²⁶ While the Register's determination is binding on the CRB in subsequent proceedings, it was unclear if it would have an effect on the rates already set through 2012.⁴¹²⁷

A partial answer came in the form of SoundExchange, Inc. v. Librarian of Congress,⁴¹²⁸ in which SoundExchange contested the CRB's 2008 rate-setting decision, arguing that the rates should be closer to 13% of royalties. The court rejected this argument, noting that the CRB's decision was not arbitrary and capricious. However, the court agreed with the Register's determination that the conflation of Section 112 and 114 rates was improper, but found that the evidence in the record was insufficient for it to set a rate, and so remanded the case to the CRB to set a royalty rate that disaggregated the Section 112 and 114 royalties.⁴¹²⁹

⁴¹²⁴ 73 Fed. Reg. 4080, 4102 (Jan. 24, 2008).

⁴¹²⁵ 73 Fed. Reg. 9143, 9146 (Feb. 19, 2008) ("Royalties collected under section 114 are paid to the performers and the copyright owners of the sound recordings, i.e., usually the record companies; whereas, the royalties collected pursuant to the section 112 license are not paid to performers."); "Copyright Office Declares Judges' Ruling on Ephemeral Rates Was Legal Error," *BNA's Patent, Trademark & Copyright Journal* (Feb. 29, 2008) at 446.

⁴¹²⁶ 17 U.S.C. § 803(c)(4); "Copyright Office Declares Judges' Ruling on Ephemeral Rates Was Legal Error," *BNA's Patent, Trademark & Copyright Journal* (Feb. 29, 2008) at 447.

⁴¹²⁷ "Copyright Office Declares Judges' Ruling on Ephemeral Rates Was Legal Error," *BNA's Patent, Trademark & Copyright Journal* (Feb. 29, 2008) at 446.

⁴¹²⁸ 571 F.3d 1220 (D.C. Cir. 2009).

⁴¹²⁹ SoundExchange, Inc. v. Librarian of Congress, 571 F.3d 1220, 1225-26 (D.C. Cir. 2009); "Copyright Royalty Judges' Rate Determination for Satellite Radio Performances Stands," *Bloomberg Law Reports – Intellectual Property*, Vol. 3, No. 30 (July 27, 2009) at 1-2.

The CRB then adopted a final rule on rates and terms for preexisting subscription services and satellite digital audio radio services, effective March 5, 2010, establishing monthly royalties for the performances equal to the following percentages of monthly gross revenues resulting from residential services in the U.S.:

- 6.0% for 2007 and 2008
- 6.5% for 2009
- 7.0% for 2010
- 7.5% for 2011
- 8.0% for 2012

Additionally, royalties for ephemeral recordings made in connection with such performances were set at 5% of the total royalties for the transmissions that they are made to facilitate (thereby differentiating the Section 112 and 114 royalties).⁴¹³⁰

On April 17, 2013, after conducting a rate determination proceeding in 2012, the CRB published its determination of the rates and terms of royalty payments payable by preexisting subscription services and SDARS under Sections 112 and 114. The CRB set the Section 114(f)(1) rates for preexisting subscription services at 8% of gross revenues for 2013 and 8.5% for 2014 through 2017. The Section 114(f)(1) rates for Sirius XM were set at 9% of gross revenues for 2013, 9.5% for 2014, 10.0% for 2015, 10.5% for 2016, and 11.0% for 2017.⁴¹³¹ The CRB further determined, pursuant to a joint stipulation of all parties to the proceeding, that the value accorded the Section 112 license was combined with that of the Section 114 license and the value is allocated 5% to the Section 112 license and 95% to the Section 114 license, consistent with the current regulations applicable to webcasters, broadcasters, SDARS, and new subscription services.⁴¹³²

In a decision also published on April 17, 2013, the Register of Copyrights determined that it was legal error for the CRB to apply the four factors set forth in Section 801(b)(1) to establish 7.5% as a benchmark royalty rate upon which to base escalating royalty rates for future years, but then not to apply (or reapply) the Section 801(b)(1) factors to each of the escalated royalty rates.⁴¹³³ In response to the Register's determination, the CRB on May 28, 2013 published a modification to its April 17, 2013 determination.⁴¹³⁴ Section 803(c)(4) authorizes the CRB to issue amendments to a written determination to correct any technical or clerical errors in the determination or to modify the terms, but not the rates, of royalty payments in response to unforeseen circumstances that would frustrate the proper implementation of such

⁴¹³⁰ 75 Fed. Reg. 5513 (Feb. 3, 2010).

⁴¹³¹ 78 Fed. Reg. 23054 (Apr. 17, 2013).

⁴¹³² *Id.* at 23056.

⁴¹³³ 78 Fed. Reg. 22913 (Apr. 17, 2013).

⁴¹³⁴ 78 Fed. Reg. 31842 (May 28, 2013). In its modification, the CRB noted, "Although the Register's decision does not changes the rates and terms set in the [April 17, 2013 determination], her opinion is binding on the Judges prospectively." *Id.* at 31843.

determination. The CRB determined that a supplemental review of the application of the Section 801(b)(1) factors was technical in nature and was therefore amenable to correction pursuant to Section 803(c)(4). Accordingly, in its modified determination, the CRB applied the Section 801(b)(1) factors specifically to the prospective escalated royalty rates, concluding that the escalated rates were appropriate under the factors and should therefore be left unchanged.⁴¹³⁵

In SoundExchange, Inc. v. Muzak LLC,⁴¹³⁶ the D.C. Circuit held that the term “service,” for purposes of the definition of “preexisting subscription service,” contemplates a double limitation – both the business entity and its program offering must qualify under the definition in order for the transmissions to be eligible for the favorable, grandfathered rate. Accordingly, only the DishCD service that Muzak was offering pre-1998 qualified for the favorable rate, and not the SonicTap service that Muzak’s parent acquired in 2012 but that was not being offered pre-1998.⁴¹³⁷ On remand, the district court adjudicated SoundExchange’s challenge to Muzak’s payment of preexisting subscription service (PSS) rates on programming provided to subscribers of a service branded as SonicTap, a service owned by a parent company that had acquired the previous provider of that service, DMX, as well as Muzak, and then consolidated that service with those provided by Muzak. The court held that the D.C. Circuit’s decision precluded any argument that Muzak could permissibly pay PSS rates for non-Dish transmissions, even if the content of the transmissions made by each brand were virtually identical, but refused summary judgment to the plaintiff on Muzak’s affirmative defense of unclean hands because of the need for discovery.⁴¹³⁸

As described in Music Choice v. Copyright Royalty Board,⁴¹³⁹ in 2016, the CRB commenced a proceeding to establish PSS royalty rates for the years 2018 to 2022. The proceeding concerned the royalty rates that Music Choice, the only remaining PSS participating, must pay to copyright holders by way of SoundExchange. Over the course of the proceeding, the CRB referred to the Register of Copyrights the legal question of whether Music Choice’s internet transmissions qualify as a PSS. The Register determined that, as a matter of law, internet transmissions are categorically excluded from the unconditional grandfathered rate (which under 17 U.S.C. §114(j)(11) applies only to the extent a PSS’s subscription transmission is made in the same transmission medium used by such service on July 31, 1998) because the DMCA’s legislative history made clear that Congress intended to limit the grandfathered rate to Music Choice’s offerings in the specific transmission media affirmatively identified in the DMCA Conference Report – cable or satellite.⁴¹⁴⁰

⁴¹³⁵ Id. at 31843-46.

⁴¹³⁶ 854 F.3d 713 (D.C. Cir. 2017).

⁴¹³⁷ Id. at *1392-93.

⁴¹³⁸ SoundExchange, Inc. v. Muzak, LLC, 322 F. Supp. 3d 72, 76-78 (D.D.C. 2018).

⁴¹³⁹ 970 F.3d 418 (D.C. Cir. 2020).

⁴¹⁴⁰ Id. at 421-22.

The Register went on to set out a non-exhaustive six-factor test to guide the CRB’s determination of whether Music Choice’s internet transmissions qualify for the conditional grandfathered rate, which applies to a transmission made by a PSS in a different transmission medium, or by a new subscription service, if it meets several additional conditions and requirements as set forth under 17 U.S.C. § 114(d)(2)(C). In its Final Determination setting rates for the 2018 to 2022 period, the CRB applied the Register’s legal opinion and excluded Music Choice’s internet transmissions from the unconditional grandfathered rate. It then applied the Register’s six-factor test to determine that Music Choice’s internet transmissions are also excluded from the conditional grandfathered rate to the extent they are available outside a subscriber’s residence, such as through mobile applications. Because Music Choice’s internet transmissions did not qualify for either grandfathered rates, they would be subject to the higher market-based royalty rate. Music Choice appealed the Final Determination.⁴¹⁴¹

The D.C. Circuit found the Register’s legal opinion to be erroneous. Under the DMCA, a subscription digital audio transmission is subject to the unconditional grandfathered rate if it is (1) made by a PSS and (2) offered in the same transmission medium used by such service on July 31, 1998. The court found that, contrary to the Register’s conclusion, neither element categorically excludes internet transmissions. First, the court noted that the DMCA’s definition of a PSS is broad enough to include internet transmissions that were in fact occurring as of July 31, 1998, because under 17 U.S.C. § 114(j)(11) it includes any “service that performs sound recordings by means of noninteractive audio-only subscription digital audio transmissions, which was in existence and was making such transmissions to the public for a fee on or before July 31, 1998.” The court noted it had held in Muzak that the term “service” in “preexisting subscription service” refers to both the business entity making the transmission (Music Choice) and to the “program offering” the entity provides (the Music Choice digital audio service). Therefore, for a digital audio transmission to qualify as a PSS, first, it must be made by a business entity that was in existence on or before July 31, 1998, and second, the relevant “program offering” must have been in existence on July 31, 1998.⁴¹⁴²

In this case, all agreed that Music Choice satisfied the first prong. The Register’s conclusion that internet transmissions are categorically excluded under the second prong was erroneous because the DMCA grandfathers a covered entity’s program offerings that were in existence on or before July 31, 1998, and it was undisputed that Music Choice had been providing some digital audio transmissions over the internet since 1996 and was still doing so on July 31, 1998. Those internet transmissions that are part of the same “service” therefore fall within the scope of the DMCA’s definition of preexisting services.⁴¹⁴³

Second, the DMCA under 17 U.S.C. § 114(d)(2)(B) applies the unconditional grandfathered rate to transmissions made “in the same transmission medium.” The text of the provision does not distinguish between different transmission media, and there is no suggestion

⁴¹⁴¹ Id. at 422.

⁴¹⁴² Id. at 425.

⁴¹⁴³ Id.

in the text that a “transmission medium” excludes internet transmission. The transmission medium clause, like the preexisting service definition, focuses on the actual preexisting entity and program offering, not the manner of transmission. The court therefore concluded that internet transmissions are subject to the unconditional grandfathered rate if they were made by a PSS on July 31, 1998.⁴¹⁴⁴

The court vacated the Register’s legal opinion and the part of the CRB’s Final Determination applying that opinion and remanded for the CRB to determine under the correct legal standard whether Music Choice’s current service offering, including its internet transmissions, qualifies for the unconditional or conditional grandfathered rates. As part of its determination, the CRB would need to assess whether Music Choice’s current internet service offerings, including its mobile application and internet-exclusive channels, were a part of the service offering Music Choice provided on July 31, 1998. The court noted that while on the record below it was undisputed that Music Choice was making some internet transmissions at that date, there was a question whether those transmissions were available outside the home.⁴¹⁴⁵

(b) Eligible Nonsubscription Services (Webcasters)

While the CARP proceedings for eligible nonsubscription services were pending, the major record labels and representatives of various FCC-licensed broadcasters reached an agreement in Dec. 2001 on royalty rates to be paid by FCC-licensed broadcasters when they simultaneously stream their AM/FM broadcasts during the period from Oct. 28, 1998 through Dec. 31, 2008.⁴¹⁴⁶ The settling parties submitted a request to the Copyright Office to withdraw from the CARP, further requesting that the Copyright Office withdraw the issue of AM/FM streaming from the CARP and publish the settled rates in the Federal Register for public comment after the CARP had delivered its report on the remaining issues in the proceeding. They requested that, if there were no objections to the published settled rates, the Librarian of Congress adopt those rates. The settling parties insisted, however, that the settled rates not be revealed to the CARP before the CARP’s determination of the royalty rates that should apply to nonsubscription digital audio transmissions other than AM/FM streaming (i.e., webcasting).⁴¹⁴⁷

The Copyright Office rejected the settling parties’ requests, noting that neither the copyright statute nor existing regulations provided for negotiation and settlement of generally applicable royalty rates after a CARP has been empaneled. The Copyright Office therefore ruled that the AM/FM streaming rate would have to be resolved in the CARP proceeding, and further

⁴¹⁴⁴ Id. at 425-26.

⁴¹⁴⁵ Id. at 427-28. The court also vacated the CRB’s amendments to the royalty audit procedures as arbitrary and capricious. Id. at 428-30.

⁴¹⁴⁶ Order, Docket No. 2000-9 CARP DTRA 1&2 (Jan. 7, 2002), at 1.

⁴¹⁴⁷ Id.

noted that the parties were free to make a joint submission to the CARP urging that it adopt the rates upon which they had agreed.⁴¹⁴⁸

The CARP issued its ruling on Feb. 20, 2002, setting the recommended performance fees at 0.14 cents per performance for webcasting to Internet listeners for free and at 0.07 cents per performance for simultaneous webcasting of AM/FM broadcasts by traditional FCC-licensed broadcasters.⁴¹⁴⁹ The CARP's recommendations were reviewed by the Copyright Office, which recommended to the Librarian of Congress that the Librarian reject the rates set forth in the CARP's report. On June 20, 2002, the Librarian published his final decision on the matter, which abandoned the CARP's two-tiered rate structure of 0.14 cents per performance for Internet-only transmissions and 0.07 cents for each retransmission of a performance in an AM/FM radio broadcast, deciding instead that the rate of 0.07 cents should apply to both types of transmission. The foregoing rates applied for the period from Oct. 28, 1998 through Dec. 31, 2002.⁴¹⁵⁰ The Register of Copyright's rationale for rejection of the CARP rates, together with the Librarian's order adopting the Register's recommendation, were published on July 8, 2003 at 67 Fed. Reg. 45239. The D.C. Circuit rejected various challenges to the Librarian's decision, allowing it to stand.⁴¹⁵¹

On Jan. 30, 2002, the Copyright Office announced the initiation of the next voluntary six-month negotiation period for determining reasonable rates and terms for eligible nonsubscription services for the 2003-2004 period.⁴¹⁵² No settlements were reached and the Copyright Office on Nov. 20, 2002 requested interested parties to file notices of intent to participate in, and written comments and proposals for the scheduling of, a CARP proceeding.⁴¹⁵³

On Dec. 4, 2002, President Bush signed into law the Small Webcaster Settlement Act of 2002 ("SWSA"), Pub. L. 107-321, 116 Stat. 2780, which amended the royalty rates to be paid for the Section 112 and Section 114 statutory licenses by an "eligible small webcaster" and by noncommercial webcasters. The SWSA is the legislative embodiment of an agreement negotiated between small webcasters and the RIAA.⁴¹⁵⁴ Among other things, the SWSA allows SoundExchange, the Receiving Agent designated by the Librarian of Congress in his June 20, 2002 order for collecting royalty payments made by eligible nonsubscription transmission

⁴¹⁴⁸ *Id.* at 1-2.

⁴¹⁴⁹ The CARP Report was available online as of Feb. 20, 2002 at www.loc.gov/copyright/carp/webcasting_rates.html.

⁴¹⁵⁰ Librarian of Congress, "Webcasting Determination," available as of June 21, 2002 at www.copyright.gov/carp/webcasting_rates_final.html.

⁴¹⁵¹ *Beethoven.com LLC v. Librarian of Congress*, 394 F.3d 939 (D.C. Cir. 2005).

⁴¹⁵² 67 Fed. Reg. 4472 (Jan. 30, 2002).

⁴¹⁵³ 67 Fed. Reg. 70093 (Nov. 20, 2002).

⁴¹⁵⁴ The agreement is published at 67 Fed. Reg. 78510 (Dec. 24, 2002).

services under the Section 112 and Section 114 statutory licenses,⁴¹⁵⁵ to enter into agreements on behalf of all copyright owners and performers to set rates, terms and conditions for eligible small webcasters operating under those statutory licenses.

Section 8(f) of the SWSA defines an “eligible small webcaster” as “a person or entity that has obtained a compulsory license under 17 U.S.C. 112 or 114 and the implementing regulations therefor to make eligible nonsubscription transmissions and ephemeral recordings that—

- (1) For the period beginning on October 28, 1998, and ending on December 31, 2002, has gross revenues during the period beginning on November 1, 1998, and ending on June 30, 2002, of not more than \$1,000,000;
- (2) For 2003, together with its affiliates, has gross revenues during 2003 of not more than \$500,000; and
- (3) For 2004, together with its affiliates, has gross revenues plus third party participation revenues and revenues from the operation of new subscription services during 2004 of not more than \$1,250,000.”⁴¹⁵⁶

The SWSA governed the period from Oct. 28, 1998 through Dec. 31, 2004. During that period, eligible small webcasters could elect to pay the royalty rates established by the SWSA rather than the statutory rates determined by any other applicable method, such as a CARP proceeding. To be eligible for the SWSA rates, an eligible small webcaster was required to submit a completed and signed election form to SoundExchange by no later than the first date on which the webcaster would have to make a royalty payment under the SWSA. Subject to certain minimum annual fees, the royalty rates under the SWSA for Oct. 28, 1998 through Dec. 31, 2002 were 8 percent of a webcaster’s gross revenues or 5 percent of its expenses, whichever is greater. For 2003 and 2004, the royalty rates were 10 percent of the webcaster's first \$250,000 in gross revenues and 12 percent of any gross revenues in excess of \$250,000 during the applicable year, or 7 percent of the webcaster's expenses during the applicable year, whichever is greater.⁴¹⁵⁷ Under Section 5 of the SWSA, the minimum annual fees ranged from \$500 to \$5,000, depending upon the year and the gross revenues of the webcaster.⁴¹⁵⁸

In June of 2003, the RIAA and educational and other tax exempt institutions reached an agreement under which college radio stations and other educational broadcast stations staffed substantially by students enrolled and the educational institution could pay even further discounted license fees for webcasting in the amount of a flat fee of \$200 annually for the years 1998 and 1999, \$250 annually for the years 2000 through 2003, and a fee of \$500 for 2004, except that educational institutions having fewer than 10,000 students could continue to pay

⁴¹⁵⁵ See 67 Fed. Reg. 45239 (July 8, 2002).

⁴¹⁵⁶ *Id.* at 78513.

⁴¹⁵⁷ *Id.* at 78511.

⁴¹⁵⁸ *Id.* at 78512.

only \$250 in 2004. The agreement allowed noncommercial webcasters at other tax exempt institutions to pay an annual fee of between \$200 and \$500, depending upon whether the webcasting is done through a single or multiple channels. The agreement applied retroactively to October 28, 1998 and lasted through the end of 2004.⁴¹⁵⁹

In May of 2003, the Digital Media Association, the American Federation of Television and Radio Artists, the American Federation of Musicians of the United States and Canada, and the RIAA, acting under the provisions of the SWSA, agreed on a proposal for royalty rates to be paid by eligible non-subscription services for the 2003 and 2004 statutory licensing period and by new subscription services from 1998 through Dec. 31, 2004 (the “SWSA Agreement”), and submitted the proposal to the Copyright Office for possible adoption without a CARP. The agreement also established proposed rates for Internet streaming of AM/FM broadcasts. On May 20, 2003, the Copyright Office published the proposal for comment, which would establish the royalty rates for each of the three categories of services set forth in the table below.⁴¹⁶⁰ On Feb. 6, 2004, the Copyright Office adopted the proposal as a final rule.⁴¹⁶¹

Eligible Non-subscription Services	Option of paying royalties as follows: <u>Per Performance Option</u> – 0.0762 cents per performance for digital audio transmissions <u>Aggregate Tuning Hour Option</u> – 1.17 cents per aggregate tuning hour for all channels and stations except channels and stations where the programming consists of non-music programming, such as news, talk, sports or business programming. For such non-music channels and stations, the licensee must pay 0.0762 cents per aggregate tuning hour. <u>Minimum Annual Fee</u>: \$2,500 <u>Ephemeral Recordings</u>: These rates will be deemed to include the royalties payable for ephemeral recordings
New Subscription Services	Options of paying royalties as follows: <u>Per Performance Option</u> – 0.0762 cents per performance for digital audio transmissions <u>Aggregate Tuning Hour Option</u> – 1.17 cents per aggregate tuning hour for all channels and stations except channels and stations where the programming consists of non-music programming, such as news, talk, sports or business programming. For such non-music channels and stations, the licensee must pay 0.0762 cents per aggregate tuning hour.

⁴¹⁵⁹ 68 Fed. Reg. 35008 (June 11, 2003).

⁴¹⁶⁰ 68 Fed. Reg. 27506 (May 20, 2003).

⁴¹⁶¹ 69 Fed. Reg. 5693 (Feb. 6, 2004).

	<u>Percentage of Subscription Revenues Option</u> – 10.9% of subscription service revenue, but in no event less than 27 cents per month for each person who subscribes. <u>Minimum Annual Fee</u> : \$2,500 <u>Ephemeral Recordings</u> : These rates will be deemed to include the royalties payable for ephemeral recordings
Internet Streaming of AM/FM Broadcasts	<u>Streaming</u> : 0.88 cents per aggregate tuning hour <u>Ephemeral Recordings</u> : The rate for ephemeral recordings by business establishment services is 10% of gross proceeds.

Webcasters wishing to take advantage of the SWSA Agreement were required to submit a completed and signed election form to SoundExchange no later than 30 days after the publication of the rates and terms in the Federal Register, or for those webcasters who had not yet made a digital audio transmission as of such publication, no later than the first date on which they would be obligated to make royalty payments.

On August 21, 2003, the Copyright Office published proposed rates and terms for noncommercial webcasters who elected not to operate under the rates and terms set under the SWSA Agreement.⁴¹⁶² Those proposed rates and terms were the same as those that were set for the period ending December 31, 2002 in the Order of the Librarian of Congress published July 8, 2002 at 67 Fed. Reg. 45239. On Feb. 6, 2004, the Copyright Office adopted the proposed rates and terms as a final rule for the 2003 and 2004 statutory licensing period.⁴¹⁶³

On June 18, 2003, the Copyright Office issued a final rule governing SoundExchange as the authorized agency to collect and distribute the statutory royalties for subscription digital transmission services and webcasting, including small webcasters.⁴¹⁶⁴ The rules governing the collection, distribution, and audit of royalties by SoundExchange may be found at 37 C.F.R. §§ 260.3 & 260.6.

As noted earlier, on Nov. 30, 2004, the Copyright Royalty and Distribution Reform Act of 2004 (“CRDRA”)⁴¹⁶⁵ was enacted, with an effective date of May 31, 2005. That Act eliminated the CARP system and replaced it with a Copyright Royalty Board (CRB) comprised of three permanent Copyright Royalty Judges (CRJs). The Act also reformed the way webcasters participate in the rate setting process. Webcasters must file a petition to participate, which costs \$150 to file, but parties with similar interests may split the cost by filing a joint petition. The CRJs provide a list of participants to all parties, who then have three months to negotiate their own royalty rates. If the parties are unable to agree, the CRJs will accept written comments

⁴¹⁶² 68 Fed. Reg. 50493 (Aug. 21, 2003).

⁴¹⁶³ 69 Fed. Reg. 5693 (Feb. 6, 2004).

⁴¹⁶⁴ 68 Fed. Reg. 36469 (June 18, 2003).

⁴¹⁶⁵ Pub. L. No. 108-419, 118 Stat. 2341 (2004).

for four to five months. These comments may include witness statements, testimony and exhibits to be presented in the proceeding, as well as other information necessary to establish terms and rates. The comment period is followed by a 60-day discovery period. Finally, the parties have one more opportunity to negotiate their own settlement at a settlement conference scheduled by the CRJs to take place outside the presence of the CRJs. Only then will the CRJs begin proceedings to set the rates.⁴¹⁶⁶

The Act also terminated the voluntary negotiation proceeding initiated by the Copyright Office in January 2004 to set rates for the 2005-2006 period for eligible nonsubscription services.⁴¹⁶⁷ On Feb. 8, 2005, as required by the Act, the Copyright Office published a notice that the rates and terms for the statutory licenses in effect on Dec. 31, 2004, for new subscription services, eligible nonsubscription services, and services exempt under Section 114(d)(1)(C)(iv), as well as the rates and terms for small webcasters published in the Federal Register under the authority of the SWSA for the years 2003-2004, would remain in effect for at least 2005.⁴¹⁶⁸ On Feb. 16, 2005, again as required by the Act, the Copyright Office published a notice initiating a proceeding, and requesting petitions to participate therein, to establish or adjust rates and terms for the statutory licenses for new subscription services and eligible nonsubscription services for the period commencing Jan. 1, 2006 through Dec. 31, 2010.⁴¹⁶⁹

After two years of testimony, on May 1, 2007, the CRB published in the Federal Register its final rule and order setting forth its decision as to the royalties that “Commercial Webcasters” (i.e., non-interactive new subscription services and eligible nonsubscription services, including simultaneous digital audio retransmissions of over-the-air AM or FM radio broadcasts) must pay to stream copyrighted music over the Internet. The new rates abandoned the existing percentage-of-revenue scheme in favor of an annual flat per-station rate structure up to a specified cap, coupled with a per-performance rate for services that exceed the cap, where “performance” is defined as the streaming of one song to one listener. The annual per-channel and per-station rate for non-commercial webcasters not exceeding 159,140 aggregate tuning hours per month and for Commercial Webcasters was set at \$500 per year. The per-performance rates for transmissions in excess of that limit by non-commercial webcasters, and for any transmissions by Commercial Webcasters, retroactive to Jan. 1, 2006, were set at:

\$0.0008 for 2006
\$0.0011 for 2007
\$0.0014 for 2008
\$0.0018 for 2009
\$0.0019 for 2010

⁴¹⁶⁶ Allison Kidd, “The Beginning of the End of the Internet Radio Royalty Dispute,” *Journal of Internet Law*, Oct. 2005, at 15, 22.

⁴¹⁶⁷ 69 Fed. Reg. 689 (Jan. 6, 2004).

⁴¹⁶⁸ 70 Fed. Reg. 6736 (Feb. 8, 2005).

⁴¹⁶⁹ 70 Fed. Reg. 7970 (Feb. 16, 2005).

These rates were inclusive of both the Section 114 license fees and the royalty payable under Section 112 for ephemeral recordings used solely to facilitate transmissions for which it paid royalties.⁴¹⁷⁰

The CRB's decision caused great controversy and protest, particularly among small webcasters, who claimed the rates were so high that they would put the webcasters out of business. Several bills were introduced in Congress and negotiations with SoundExchange took place to reduce the rates for small webcasters. On May 22, 2007 SoundExchange announced that it would extend for another three years (through 2010) the previous, lower rates under the SWSA for small webcasters (i.e., 10% of gross revenue up to \$250,000 and 12% of revenue exceeding that amount).⁴¹⁷¹ On Aug. 21, 2007, SoundExchange set out certain conditions that had to be met by a small webcaster to qualify for the favorable rates – the webcaster had to earn less than \$1.2 million in total annual revenue and could not exceed a total of 5 million aggregate tuning hours each month. Should the threshold be exceeded, the webcaster would be required to pay the CRB's published rates. SoundExchange announced that the agreement would apply only to performance royalties collected on behalf of the 20,000 recording artists and 3,500 record labels represented by the collective – royalties due to other artists and labels would be payable under the CRB's rates. Interested webcasters had until Sept. 14, 2007 to accept the offer.⁴¹⁷²

On Aug. 23, 2007, SoundExchange also announced an accord on the amount of fees some large webcasters would pay – specifically, that a \$50,000 cap would replace the \$500 per-station minimum fee set by the CRB. In return for the cap, the signatory webcasters agreed within six months to begin collecting and reporting census information on all songs streamed over the Internet. SoundExchange and DiMA also agreed to form a committee designed to analyze the issue of audio stream-ripping and technological solutions that might be available. The agreement did not, however, disturb the CRB's per-performance royalty fees.⁴¹⁷³

On Aug. 10, 2007, the Copyright Office, acting under the provisions of the CRDRA, formally terminated all open proceedings under the old CARP system.⁴¹⁷⁴

⁴¹⁷⁰ 72 Fed. Reg. 24084, 24111 (May 1, 2007). The CRB's decision was initially set forth in a report published on its web site on Mar. 2, 2007. Representatives of the Intercollegiate Broadcasting System Inc., DiMA, National Public Radio, the Radio Broadcasters, Royalty Logic Inc., WHRB (FM), SoundExchange, and many small commercial webcasters filed a series of motions seeking a rehearing on the royalty scheme. On April 16, 2007, the CRB rejected the motions. On July 11, 2007, the U.S. Court of Appeals for the D.C. Circuit denied a petition filed by webcasters seeking to stay the CRB's determination. "SoundExchange Offers Webcasters Reprieve After D.C. Court Denies Petition to Stay," *BNA's Patent, Trademark & Copyright Journal* (July 20, 2007) at 345.

⁴¹⁷¹ *Id.*

⁴¹⁷² "SoundExchange Agrees to Separate Royalty Deals Between Large and Small Webcasters," *BNA's Patent, Trademark & Copyright Journal* (Aug. 31, 2007) at 530.

⁴¹⁷³ *Id.* at 529.

⁴¹⁷⁴ 72 Fed. Reg. 45071 (Aug. 10, 2007).

On Oct. 16, 2008, President Bush signed into law the Webcaster Settlement Act of 2008 (“WSA 2008”), Pub. L. 110-435, 122 Stat. 4974, in order to provide more time for SoundExchange and webcasters to come up with an agreement on royalty rates. Modifying Section 114(f)(5), the WSA 2008 granted SoundExchange the authority to make settlements until Feb. 15, 2009, and allowed any agreement reached to have terms in force until the end of 2016. It also eliminated all mentions of “small webcaster,” replacing it with simply “webcaster,” thereby allowing webcasters of any size to enter into negotiated agreements. The WSA 2008 further allowed the parties to agree that their alternative rates may be drawn on as precedent in future rate-setting proceedings, and also made optional the requirements for what shall be included in such agreements.⁴¹⁷⁵

In January 2009, the Corporation for Public Broadcasting and SoundExchange came to an agreement establishing royalties to be paid on behalf of public radio systems for streaming sound recordings on about 450 public radio web sites from 2005 through 2010. The agreement provides SoundExchange with a single up-front payment of \$1.85 million, along with consolidated usage and playlist information to assist with the process of compensating individual artists. Additionally, National Public Radio agreed to withdraw its appeal of a May 2007 CRB rate decision.⁴¹⁷⁶ Several weeks later, in February, the National Association of Broadcasters also reached an agreement with SoundExchange to lower the Internet broadcasting rates for participating radio stations by about 16% in 2009 and 2010, with stations paying an annual fee of \$500 for each channel and a per-performance royalty rate of \$0.0008 in 2006, increasing to \$0.0025 in 2015, with a ceiling of \$50,000.⁴¹⁷⁷ A group of small webcasters, including Attention Span Radio, Blogmusik, Born Again Radio, Music Justice, My Jazz Network, and Voice of Country, also came to an agreement with SoundExchange that covered 2006 through 2015. Under the agreement, transmissions cannot exceed 5 million tuning hours per month, and the rates are calculated as either:

(1) the greater of 10% of the webcaster’s first gross revenue in excess of \$250,000, or 12% of any annual gross revenue exceeding \$250,000; or

(2) 7% of the webcaster’s annual expenses. For transmissions exceeding 5 million tuning hours per month, the rates are either those set by the CRB’s 2007 determination, or whichever rates are then applicable under Sections 112(e) and 114.⁴¹⁷⁸

⁴¹⁷⁵ “Congress Votes to Allow Webcasters To Negotiate Rates With Sound Exchange,” *BNA’s Patent, Trademark & Copyright Journal* (Oct. 3, 2008) at 753.

⁴¹⁷⁶ “Public Broadcasters Agree to Web Music Royalties” (Jan. 15, 2009), available as of Aug. 1, 2012 at <http://www.lexisnexis.com/community/copyright-trademarklaw/blogs/newsheadlines/archive/2009/01/16/public-broadcasters-agree-to-web-music-royalties.aspx>.

⁴¹⁷⁷ Rachel Metz, “Agreement Reached on Internet Music Royalty Rates,” *The Washington Post*, Feb. 17, 2009; 74 Fed. Reg. 9293, 9300 (Mar. 3, 2009).

⁴¹⁷⁸ 74 Fed. Reg. 9293 (Mar. 3, 2009).

The Webcaster Settlement Act of 2008 was amended in 2009 to extend the negotiation period, and President Obama signed it into law on June 30, 2009. After two years of negotiations, on July 7, 2009, SoundExchange and “pureplay” webcasters (businesses whose primary form of business is streaming sound recordings under a government license) came to an agreement on music royalties. Web sites with revenue below \$1.25 million agreed to pay 12-14% of their revenue in royalties annually, along with an annual \$25,000 fee (applied to the royalties owed). The agreement covers the period of 2006 through 2015 for large web sites, or 2006 through 2014 for small web sites.⁴¹⁷⁹

The CRB’s 2007 determination of rates was challenged in Intercollegiate Broadcast Systems Inc. v. Copyright Royalty Board.⁴¹⁸⁰ The court largely upheld the determination, ruling that the CRB’s interpretation of Section 114 was not unreasonable for failing to assume a perfectly competitive market; that commercial webcasters had failed to show that the rates were “crushing and disproportionate” (and therefore arbitrary and capricious); and that the CRB was justified in determining a per-performance rate, rather than a percentage of revenue fee structure for small webcasters. However, because webcasters’ services could arguably be seen as offering thousands of channels, the court remanded the question of whether the CRB should cap minimum annual fees for a single licensee, rather than basing such fees on a per-channel-per-station basis. The court also remanded the issue posed by the \$500 minimum fees for noncommercial webcasters, because the court said it was not supported by sufficient evidence in the record.⁴¹⁸¹

Following Intercollegiate Broadcast Systems, the CRB established a comment period in November 2009 for the parties to reach an agreement regarding the remanded minimum annual fee issue, and on Dec. 2 SoundExchange and DiMA submitted a settlement. The settlement was published for comment on Dec. 23,⁴¹⁸² and soon after adopted as final, setting the minimum annual fee for commercial webcasters at \$500 for 2006-2010.⁴¹⁸³ The second issue on remand, concerning the \$500 fee for noncommercial broadcasters, was settled by the CRB in a Sept. 17 decision in favor of upholding the fee. The CRB ruled that the evidence presented on remand supported at least a \$500 minimum fee for noncommercial webcasters, and that the industry demonstrated an acceptance of these minimum fees, as evidenced in the agreements that industry representatives have entered into pursuant to the Webcaster Settlement Acts of 2008 and 2009.⁴¹⁸⁴

⁴¹⁷⁹ Nathan Pollard, “SoundExchange and ‘Pureplay’ Webcasters Reach Royalty Agreement,” *BNA News* (July 9, 2009).

⁴¹⁸⁰ 571 F.3d 69 (D.C. Cir. 2009).

⁴¹⁸¹ *Id.* at 76-82.

⁴¹⁸² 74 Fed. Reg. 68214 (Dec. 23, 2009).

⁴¹⁸³ 75 Fed. Reg. 6097 (Feb. 8, 2010).

⁴¹⁸⁴ 75 Fed. Reg. 56873 (Sept. 17, 2010).

The CRB then convened a hearing to determine the rates and terms applicable to the non-settling participants and published a final determination on Mar. 9, 2011.⁴¹⁸⁵ One of the participants filed an appeal to the D.C. Circuit, challenging both the \$500 minimum fee imposed and the constitutionality of the judges under the Appointments Clause of the Constitution. On July 6, 2012, the D.C. Circuit ruled that the CRB judges were acting as principal officers of the United States government in violation of the Appointments Clause of the Constitution.⁴¹⁸⁶ To cure the violation of the Appointments Clause, the court excised that portion of the Act establishing the CRB that limited the Librarian of Congress' ability to remove judges. Having determined that the judges were not validly appointed at the time they issued the challenged determination, the D.C. Circuit vacated and remanded the determination, so that a constitutionally appointed panel of judges could render a new determination.⁴¹⁸⁷

On remand, the CRB reviewed the entire record in the proceeding *de novo*, and on Apr. 25, 2014 published its determination of rates and terms for digital performances of sound recordings and the making of ephemeral recordings by webcasters for the period from Jan. 1, 2011 through Dec. 31, 2015.⁴¹⁸⁸ Specifically, the CRB determined that for commercial webcasters subject to the agreement between the National Association of Broadcasters and SoundExchange, the rates would be as stipulated in that agreement. For all other commercial webcasters, the rates would be:

<u>Year</u>	<u>Rate per performance</u>
2011	\$0.0019
2012	\$0.0021
2013	\$0.0021
2015	\$0.0023

For noncommercial educational webcasters, rates would be as agreed by and between College Broadcasters, Inc. and SoundExchange in the agreement approved by the judges in this proceeding.⁴¹⁹⁰ For other noncommercial webcasters, the rate would be \$500 per station or channel, including side channels, up to a maximum usage of 159,140 Aggregate Tuning Hours

⁴¹⁸⁵ 76 Fed. Reg. 13026 (Mar. 9, 2011).

⁴¹⁸⁶ Intercollegiate Broadcasting Sys. v. Copyright Royalty Board, 684 F.3d 1331, 1342 (D.C. Cir. 2012), cert. denied, 133 S. Ct. 2735 (2013).

⁴¹⁸⁷ Id. at 1334, 1342.

⁴¹⁸⁸ 79 Fed. Reg. 23102 (Apr. 25, 2014).

⁴¹⁸⁹ This rate is applicable from first performance, but subject to recoupment credit for the agreed minimum fee of \$500 per year for each station or channel. Id. at 23102.

⁴¹⁹⁰ The terms of that agreement, which was first published by the Copyright Office at 74 Fed. Reg. 40616 (Aug. 12, 2009), provide for an annual, nonrefundable minimum fee of \$500 for each station or individual channel, including each of its individual side channels. Those educational webcasters whose monthly Aggregate Tuning Hours exceed 159,140 per month pay additional fees on a per-performance basis. The agreement also provides for an optional \$100 proxy fee that noncommercial educational webcasters may pay in lieu of submitting reports of use of sound recordings. 79 Fed. Reg. at 23120.

per month. Commercial usage rates would apply to usage in excess of 159,140 hours per month. All parties in interest in the proceeding agreed that royalties payable for the Section 112(e) license should be bundled with the Section 114 royalties and deemed to be 5% of the bundled remittances.⁴¹⁹¹

On Oct. 31, 2014, the CRB, after a *de novo* review of its previous setting of the minimum annual fee for noncommercial webcasters at \$500 for 2006-2010 (the *de novo* review being necessitated by the D.C. Circuit's ruling that the judges had not been validly appointed at the time they issued the initial determination), announced its final determination upholding the validity and application of the \$500 minimum fee for noncommercial webcasters for the licensing period 2006 through 2010.⁴¹⁹²

On Aug. 11, 2015, the D.C. Circuit rejected challenges by Intercollegiate Broadcasting to the decisions of the CRB on remand. The court found that the CRB decisions were not invalid on the grounds that they were allegedly tainted by the previous Board's reasoning (even though the new Board reached an identical result), and rejected various challenges to the merits of the decisions.⁴¹⁹³

In U.S. v. American Society of Composers, Authors and Publishers,⁴¹⁹⁴ the U.S. District Court for the Southern District of New York set the licensing rates and terms that AOL, RealNetworks, and Yahoo! would have to pay in order to publicly perform ASCAP songs over the Internet. The three companies had applied to ASCAP for a blanket license to perform ASCAP-reparatory music over the Internet, but were unable to reach an agreement, so ASCAP petitioned the court for a determination of reasonable royalty rates. Although ASCAP initially claimed that royalty rates should apply to both streaming music and downloads, an earlier proceeding determined that royalty rates should apply only to streaming music because downloads invoke the copyright holder's reproduction right, not the public performance right.⁴¹⁹⁵ The final rates involved a three-step computation, starting with a calculation of each company's domestic revenue. Because AOL and Yahoo! offer a variety of services, the domestic revenue figure is then reduced by a "music-use-adjustment" fraction (the total number of hours music is streamed to users by that company, divided by the total number of hours that visitors utilize the site, as determined by the third-party traffic measurement firm comScore Media

⁴¹⁹¹ Id. at 23102.

⁴¹⁹² 79 Fed. Reg. 64669 (Oct. 31, 2014).

⁴¹⁹³ Intercollegiate Broadcasting Sys. v. Copyright Royalty Board, 796 F.3d 111 (D.C. Cir. 2015).

⁴¹⁹⁴ 559 F. Supp. 2d 332 (S.D.N.Y. 2008).

⁴¹⁹⁵ U.S. v. American Society of Composers, Authors and Publishers, 485 F. Supp. 2d 438 (S.D.N.Y. 2007); "Court Sets Music Royalty Rate, Terms Through 2009 for Three Online Services," *BNA's Electronic Commerce & Law Report* (May 7, 2008) at 623.

Metrix). Finally, a 2.5% royalty rate is applied to the remaining revenue figure, producing the royalty rate.⁴¹⁹⁶

Noncommercial Educational Webcasters. On Sept. 28, 2015, the CRB published final regulations setting royalty rates and terms under Sections 112 and 114 for the digital performance of sound recordings by certain noncommercial educational webcasters (NEWs) and for the making of ephemeral recordings to facilitate transmission of those performances. The rates reflected a settlement between SoundExchange, Inc. and College Broadcasters, Inc. The negotiated rates apply to the period from Jan. 1, 2016 through Dec. 31, 2020. Under the settlement, an eligible NEW pays a \$500 annual fee for each of the individual channels, side channels, or stations through which it makes eligible transmissions. The \$500 fee also serves as the minimum fee for eligible NEWs. All other NEWs pay the royalties established under Part 380 Subpart A applicable to noncommercial webcasters. To qualify for the rates under the settlement, a NEW's total monthly per-channel or per-station transmissions must remain below 159,140 aggregate tuning hours (ATH). If a NEW's transmissions exceed that threshold, the NEW must pay royalties for the relevant month, and for the remainder of the relevant year, in accordance with the otherwise applicable noncommercial rates determined in the proceeding. In subsequent years, a NEW that wishes to pay the rates under the settlement must take affirmative steps not to exceed the 159,140 ATH threshold. NEWs with limited listenership may pay a \$100 proxy fee to avoid the burden of census reporting. The settlement increases the listenership cap from 55,000 ATH to 80,000 ATH for services electing the proxy fee in lieu of the census reporting option.⁴¹⁹⁷

(c) New Subscription Services

On Feb. 12, 2001, the Copyright Office announced the initiation of the six-month statutory voluntary negotiation period for determining reasonable rates and terms for the statutory license for new subscription services.⁴¹⁹⁸ No agreements were reached. After the close of the negotiation period, the Copyright Office received petitions requesting that a CARP be convened to establish terms and rates for the statutory license covering new subscription services. The petitioners also requested that the Copyright Office consolidate the proceeding for new subscription services with the proceeding for pre-existing satellite digital audio radio services and pre-existing subscription services.⁴¹⁹⁹ As discussed in the previous subsection, in May of 2003, the Digital Media Association, the American Federation of Television and Radio Artists, the American Federation of Musicians of the United States and Canada, and the RIAA agreed on a proposal for royalty rates to be paid by new subscription services for the period from 1998 through Dec. 31, 2004, and submitted the proposal to the Copyright Office for

⁴¹⁹⁶ "Court Sets Music Royalty Rate, Terms Through 2009 for Three Online Services," *BNA's Electronic Commerce & Law Report* (May 7, 2008) at 623-4.

⁴¹⁹⁷ 80 Fed. Reg. 58201 (Sept. 28, 2015).

⁴¹⁹⁸ 66 Fed. Reg. 9881 (Feb. 12, 2001).

⁴¹⁹⁹ 66 Fed. Reg. 58180 (Nov. 20, 2001).

possible adoption without a CARP. On May 20, 2003, the Copyright Office published the proposal for comment.⁴²⁰⁰ On Feb. 6, 2004, the Copyright Office adopted the proposal as a final rule.⁴²⁰¹

As noted in the previous subsection, on Nov. 30, 2004, the Copyright Royalty and Distribution Reform Act of 2004⁴²⁰² was enacted, with an effective date of May 31, 2005. That Act eliminated the CARP system and replaced it with three permanent Copyright Royalty Judges. In addition, the Act terminated the voluntary negotiation proceeding initiated by the Copyright Office in February 2004 to set rates for the 2005-2006 period for new subscription services.⁴²⁰³ On Feb. 8, 2005, as required by the Act, the Copyright Office published a notice that the rates and terms for the statutory licenses in effect on Dec. 31, 2004, for new subscription services, eligible nonsubscription services, and services exempt under Section 114(d)(1)(C)(iv), as well as the rates and terms for small webcasters published in the Federal Register under the authority of the SWSA for the years 2003-2004, would remain in effect for at least 2005.⁴²⁰⁴ On Feb. 16, 2005, again as required by the Act, the Copyright Office published a notice initiating a proceeding, and requesting petitions to participate therein, to establish or adjust rates and terms for the statutory licenses for new subscription services and eligible nonsubscription services for the period commencing Jan. 1, 2006.⁴²⁰⁵

After two years of testimony, on May 1, 2007, the CRB published in the Federal Register its final rule and order setting forth its decision as to the royalties that non-interactive new subscription services must pay to stream copyrighted music over the Internet for the period 2006 through 2010. The details of that decision are set forth in the preceding subsection.

On Oct. 31, 2005, XM Satellite Radio, Inc., filed a Petition to Initiate and Schedule Proceeding for a “new type of subscription service [which] performs sound recordings on digital audio channels programmed by the licensee for transmission by a satellite television distribution service to its residential customers, where the audio channels are bundled with television channels as part of a ‘basic’ package of service and not for a separate fee.”⁴²⁰⁶ The CRB published a notice in the Federal Register on Dec. 5, 2005 announcing commencement of the proceedings to set rates and terms for the royalty payments under Sections 112 and 114 for the activities of the new subscription service described in the XM Petition and soliciting interested parties to participate.⁴²⁰⁷ Sirius Satellite Radio, Inc. (“Sirius”), XM, MTV Networks (“MTV”), and

⁴²⁰⁰ 68 Fed. Reg. 27506 (May 20, 2003).

⁴²⁰¹ 69 Fed. Reg. 5693 (Feb. 6, 2004).

⁴²⁰² Pub. L. No. 108-419, 118 Stat. 2341 (2004).

⁴²⁰³ 69 Fed. Reg. 5196 (Feb. 3, 2004).

⁴²⁰⁴ 70 Fed. Reg. 6736 (Feb. 8, 2005).

⁴²⁰⁵ 70 Fed. Reg. 7970 (Feb. 16, 2005).

⁴²⁰⁶ 72 Fed. Reg. 72253 (Dec. 20, 2007).

⁴²⁰⁷ 70 Fed. Reg. 72471 (Dec. 05, 2005).

SoundExchange, Inc petitioned to participate, and the parties reached a settlement, with the proposed rates and terms filed on Oct. 30, 2007.⁴²⁰⁸ On Nov. 9, 2007, the CRB published a Notice of Proposed Rulemaking requesting comment on the proposed rates and terms submitted to the CRB, and adopted the proposed rates and terms in its final regulations on Dec. 20, 2007.⁴²⁰⁹

The final rates for stand-alone contracts⁴²¹⁰ are the greater of 15% of revenue, or the following monthly minimum payment per subscriber:

\$0.0075 from inception through 2006
\$0.0075 for 2007
\$0.0075 for 2008
\$0.0125 for 2009
\$0.0150 for 2010

For bundled contracts,⁴²¹¹ the final rates are the greater of 15% of revenue allocated to reflect the objective value of the licensee's service, or the following monthly minimum payment per subscriber:

\$0.0220 from inception through 2006
\$0.0220 for 2007
\$0.0220 for 2008
\$0.0220 for 2009
\$0.0250 for 2010

These rates also include a minimum, non-refundable, annual fee of \$100,000, credited against royalties due in that year. The CRB ruled that these rates were inclusive of the Section 112 ephemeral license, but declined to ascribe any particular percentage of the Section 114 royalty as representative of the value of the Section 112 license.⁴²¹²

As mentioned above in the section on preexisting subscription services, the Register of Copyrights issued a determination on Feb. 19, 2008 that stated that the CRB had committed clear legal error by failing to set separate values for the Section 112 and Section 114 licenses,

⁴²⁰⁸ 72 Fed. Reg. 72253 (Dec. 20, 2007).

⁴²⁰⁹ Id.

⁴²¹⁰ "Stand-alone contracts" mean contracts between the licensee and a cable or satellite television provider in which the service is the only content licensed by the licensee to the provider. See 72 Fed. Reg. 72253, 72255 (Dec. 20, 2007).

⁴²¹¹ "Bundled contracts" mean contracts between the licensee and a cable or satellite television provider in which the service is not the only content licensed by the licensee to the provider. 72 Fed. Reg. 72253, 72255 (Dec. 20, 2007).

⁴²¹² Id.

and including a minimum fee for the Section 112 license.⁴²¹³ Soon after, in SoundExchange, Inc. v. Librarian of Congress,⁴²¹⁴ the court agreed with the Register's determination that the conflation of Section 112 and 114 rates was improper, but found that the evidence in the record was insufficient for it to set a rate, and so remanded the case to the CRB to set a royalty rate that disaggregated the Section 112 and 114 royalties.⁴²¹⁵

In January 2009, the CRB commenced another rate determination process for new subscription services for the license period 2011-2015,⁴²¹⁶ and petitions to participate were received from SoundExchange, Royalty Logic, and Sirius XM Radio. The parties reached a settlement in late 2009, and on Jan. 22, 2010, the CRB published a notice seeking comments on the rates proposed by the settlement.⁴²¹⁷ Having received no comments or objections, the CRB adopted the proposed rates as final, amending 37 C.F.R. 383.⁴²¹⁸ The final rates for stand-alone contracts are the greater of 15% of revenue, or the following monthly minimum payment per subscriber:***

\$0.0155 for 2011
\$0.0159 for 2012
\$0.0164 for 2013
\$0.0169 for 2014
\$0.0174 for 2015

For bundled contracts, the final rates are the greater of 15% of revenue allocated to reflect the objective value of the licensee's service, or the following monthly minimum payment per subscriber:

\$0.0258 for 2011
\$0.0265 for 2012
\$0.0273 for 2013
\$0.0281 for 2014
\$0.0290 for 2015

⁴²¹³ 73 Fed. Reg. 9143, 9146 (Feb. 19, 2008) ("Royalties collected under section 114 are paid to the performers and the copyright owners of the sound recordings, i.e., usually the record companies; whereas, the royalties collected pursuant to the section 112 license are not paid to performers."); "Copyright Office Declares Judges' Ruling on Ephemeral Rates Was Legal Error," *BNA's Patent, Trademark & Copyright Journal* (Feb. 29, 2008) at 446.

⁴²¹⁴ 571 F.3d 1220 (D.C. Cir. 2009).

⁴²¹⁵ SoundExchange, Inc. v. Librarian of Congress, 571 F.3d 1220 (D.C. Cir. 2009); "Copyright Royalty Judges' Rate Determination for Satellite Radio Performances Stands," *Bloomberg Law Reports – Intellectual Property*, Vol. 3, No. 30 (July 27, 2009) at 1-2.

⁴²¹⁶ 74 Fed. Reg. 319 (Jan. 5, 2009).

⁴²¹⁷ 75 Fed. Reg. 3666 (Jan. 22, 2010).

⁴²¹⁸ 75 Fed. Reg. 14074, 14075 (Mar. 24, 2010).

In response to the Register of Copyrights' Feb. 19 2009 decision requiring that Section 112 and 114 royalties be disaggregated, the new rates also state that the royalty for Section 112(e) constitutes 5% of the total royalty payments under this agreement.⁴²¹⁹ Finally, the recordkeeping provisions of this agreement do not require licensees to report their performances.⁴²²⁰

3. The Digital Performance Right – What Constitutes an “Interactive” Service

The Section 114 statutory license does not apply to an “interactive service.” Section 114(j)(7) defines an “interactive service” as a service “that enables a member of the public to receive a transmission of a program specially created for the recipient, or on request, a transmission of a particular sound recording, whether or not as part of a program, which is selected by or on behalf of the recipient.” Section 114(j)(7) further provides that the “ability of individuals to request that particular sound recordings be performed for reception by the public at large, or in the case of a subscription service, by all subscribers of the service, does not make a service interactive, if the programming on each channel of the service does not substantially consist of sound recordings that are performed within 1 hour of the request or at a time designated by either the transmitting entity or the individual making such request. If an entity offers both interactive and noninteractive services (either concurrently or at different times), the noninteractive component shall not be treated as part of an interactive service.”

As might be expected, considerable controversy has arisen over the application of the definition of “interactive service.” A number of lawsuits have been filed involving the issue:

– On May 24, 2001, ten recording companies sued Launch Media, Inc. for copyright infringement, alleging that Launch's LAUNCHcast service created an interactive radio station by providing users with the ability to select specific artists, to rate artists and recordings, to select certain music that the user had or had not previously rated, to permanently block particular recordings, to skip the current recording and move on to the next one, and to pause the current recording and resume from the same point later.⁴²²¹ This lawsuit eventually led to a decision by the Second Circuit on the meaning of an “interactive” service, discussed in subsection (a) below.

– On June 1, 2001, Launch and other online webcasters, acting through the Digital Media Association (DiMA), filed a declaratory judgment action against the RIAA, seeking a declaration that their webcasting services were eligible for the statutory license because the songs played “ultimately are generated by a computer in a manner designed to ensure compliance with the DMCA's statutory license provision”; users “do not determine the particular sound recordings or the particular artists which become the basis of the transmission; and [they] have no ability to select or obtain advance knowledge as to the particular songs that are streamed on the

⁴²¹⁹ *Id.*

⁴²²⁰ *Id.* at 14076.

⁴²²¹ Hillel Parness, “Internet Radio: As RIAA and DiMA Prepare to Do Battle over ‘Interactivity,’ Questions Resurface About ISP Liability,” *Cyberspace Lawyer*, July/August 2001, at 2, 4.

stations”; “[a]rtist identification on the services is representative only”; the “skip” function on the services operates only forward and users “can never know which song they are ‘skipping forward to’”; and “[i]n all cases the consumer-influenced situations are available to every member of the general public.”⁴²²² The United States District Court for the Southern District of New York denied the parties’ cross-motions for dismissal under F.R.C.P. 12(b)(6) and summary judgment.⁴²²³ Launch was later acquired by Yahoo, and settled with a number of the record companies.⁴²²⁴

– On June 8, 2001, the record companies responded with three lawsuits against XACT Radio, Musicmatch, Inc., and MTVi Group, each of which provided consumers with access to streamed music over the Internet, asserting against each the same basic allegations as contained in the complaint against Launch. The complaint asserted that the use of the “skip” button by users will cause the defendants to exceed the performance complement restrictions.⁴²²⁵ Musicmatch subsequently settled its lawsuit with the record companies.

Previously, on April 17, 2000, DiMA had sought to resolve the issues in the Copyright Office, filing a rulemaking petition that sought adoption of the following proposed rule concerning the definition of a “Service” for purposes of the statutory license:

A Service making transmissions that otherwise meet the requirements for the section 114(f) statutory license is not rendered “interactive,” and thus ineligible for the statutory license, simply because the consumer may express preferences to such Service as to the musical genres, artists and sound recordings that may be incorporated into the Service’s music programming to the public. Such a Service is not “interactive” under section 114(j)(7), as long as: (i) Its transmissions are made available to the public generally; (ii) the features offered by the Service do not enable the consumer to determine or learn in advance what sound recordings will be transmitted over the Service at any particular time; and (iii) its transmissions do not substantially consist of sound recordings performed within one hour of a request or at a time designated by the transmitting entity or the individual making the request.⁴²²⁶

The Copyright Office denied the petition, ruling, among other things, that “[i]n light of the rapidly changing business models emerging in today’s digital marketplace, no rule can accurately draw the line demarcating the limits between an interactive service and a noninteractive service. Nor can one readily classify an entity which makes transmissions as exclusively interactive or

⁴²²² Id.

⁴²²³ See Arista Records, LLC v. Launch Media, Inc., 578 F.3d 148, 150 (2d Cir. 2009).

⁴²²⁴ Brad King, “Yahoo Launches Into Web Music” (June 28, 2001), available as of Feb. 22, 2002 at www.wired.com/news/mp3/0,1285,44884,00.html.

⁴²²⁵ Parness, supra note 4221, at 4.

⁴²²⁶ 65 Fed. Reg. 77330, 77331 (Dec. 11, 2000).

noninteractive.”⁴²²⁷ The Office concluded that the determination of whether a particular activity is “interactive” must be determined on a case by case basis upon a full evidentiary record.⁴²²⁸

(a) Arista Records v. Launch Media

In Arista Records, LLC v. Launch Media, Inc.,⁴²²⁹ the Second Circuit, affirming a jury determination, held that the LAUNCHcast webcasting service was not an “interactive” service within the meaning of Section 114(j)(7) as a matter of law,⁴²³⁰ and Launch Media could therefore rely on the statutory license for public performances via digital audio transmissions. The LAUNCHcast service enabled a user to create “stations” that played songs within a particular genre or similar to a particular artist or song the user selected. Specifically, upon registering with the service, the user would select artists whose music she preferred. The user would then list genres the user enjoyed and rate them on a scale. The user was also asked the percentage of songs the user had not previously rated the user would like to incorporate into the user’s station (the “unrated quota”). The minimum unrated quota was 20%. Once LAUNCHcast began playing music based on the user’s preferred artists and genres, the user would rate the songs, artists, and albums played between zero and 100. Below the rating field were hyperlinks termed “history,” “share,” and “buy.” The history hyperlink allowed the user to see a list of the songs previously played, and the buy hyperlink facilitated the user’s purchase of the songs. The share hyperlink allowed the user to share the station with other users. That feature facilitated the subscription of one user to another user’s station. While a song played, the user had the ability to pause the song, skip the song, or delete the song from the station by rating it zero. The user was not able to go back to restart a song that was playing, or to repeat any of the previously played songs in the playlist.⁴²³¹

Each time the user logged into the LAUNCHcast service and selected a station, the service generated a playlist of 50 songs selected from a hashtable of potential songs that could be put into the playlist. The hashtable was generated using a very complicated algorithm that took into account numerous variables, only some of which included the user’s preferred artists and genres and unrated quota.⁴²³² Although the playlist generated each time a user selected a radio station was unique to that user at that particular time, the Second Circuit determined that the playlist was not “specially created for the recipient” via an interactive service within the meaning of Section 114(j)(7). Based on an extensive review of the legislative history of Section 114(j)(7), the court noted that Congress’ primary concern both in creating a performance right in digital audio transmissions and in excluding interactive services from the statutory performance license was to protect sound recording copyright holders from diminution in record sales. Congress believed

⁴²²⁷ Id. at 77332-33.

⁴²²⁸ Id. at 77332.

⁴²²⁹ 578 F.3d 148 (2d Cir. 2009), cert. denied, 130 S. Ct. 1290 (2010).

⁴²³⁰ The court ruled that the issue of interactivity presents an issue of law. Id. at 151-52.

⁴²³¹ Id. at 157-58.

⁴²³² Id. at 158-59.

that interactive services, by providing predictability based on choices by the user, could approximate the predictability the music listener seeks when purchasing music, thereby diminishing music sales. The Second Circuit therefore concluded that the touchstone of an interactive service is whether it is generating playlists specially created for the recipient that have sufficient predictability to the user that the user's willingness to purchase music will be diminished.⁴²³³

The Second Circuit decided that the methodology used to select the playlists did not provide the user sufficient control to make the playlists so predictable that the user would choose to listen to the webcast in lieu of purchasing music:

First, the rules governing what songs are pooled in the hashtable ensure that the user has almost no ability to choose, let alone predict, which specific songs will be pooled in anticipation for selection to the playlist. At least 60% of the songs in the hashtable are generated by factors almost entirely beyond the user's control. The playlist – a total of fifty songs – is created from a pool of approximately 10,000 songs, at least 6,000 of which (1,000 of the most highly rated LAUNCHcast songs among all users and 5,000 randomly selected songs) are selected without any consideration for the user's song, artist, or album preferences. The user has control over the genre of songs to be played for 5,000 songs, but this degree of control is no different from a traditional radio listener expressing a preference for a country music station over a classic rock station. LAUNCHcast generates this list with safeguards to prevent the user from limiting the number of songs in the list eligible for play by selecting a narrow genre. Also, no more than 20% of the songs the user rates – marked by LAUNCHcast as explicitly rated – can be pooled in the hashtable, and no more than three times the number of explicitly rated songs divided by the total number of rated songs can be in the hashtable. This ensures that a limited number of explicitly rated songs will eventually be selected for the playlist. Ironically, this effectively means that the more songs the user explicitly rates, the less the user can predict which explicitly rated songs will be pooled in the hashtable and played on the playlist.

Second, the selection of songs from the hashtable to be included in the playlist is governed by rules preventing the user's explicitly rated songs from being anywhere near a majority of the songs on the playlist. At minimum, 20% of the songs played on the station are unrated – meaning the user has never expressed a preference for those songs. If the user attempts to increase her chances of hearing a particular song by rating only a small number of songs – making the user's list of explicitly and implicitly rated songs smaller than 100 – 90% of the songs LAUNCHcast selects for the playlist will be unrated, flooding the playlist with songs for which the user has never expressed a preference.⁴²³⁴

⁴²³³ Id. at 161.

⁴²³⁴ Id. at 162-63 (footnotes omitted).

The court further noted that even the ways in which songs were rated included variables beyond the user's control. For example, the ratings by all of the user's subscribed-to stations were included in the playlist selection process. When the user rated a particular song, LAUNCHcast then implicitly rated all other songs by that artist, subjecting the user to many songs the user may have never heard or did not even like. In addition, a user who heard a song she liked and wanted to hear again could not do so by logging off and back on to reset the station to disable the restriction against playing the same song twice on a playlist. Even if the user logged off then back on and selected the same station, the user would still hear the remainder of the playlist to which she had previously been listening with its restrictions still in operation, at least until the user had listened to at least 42 of the playlist's songs. LAUNCHcast also did not enable the user to view the unplayed songs in the playlist, ensuring that a user could not sift through a playlist to choose the songs the user wished to hear. In short, the only thing a user could control was to ensure not hearing a particular song on a particular station again by rating it zero. But the court noted that the ability not to listen to a particular song was not a violation of a copyright holder's right to be compensated when the sound recording was played.⁴²³⁵ Accordingly, the court ruled that, as a matter of law, the LAUNCHcast service was not an interactive service.⁴²³⁶

4. The Reproduction Right – Mechanical Licenses and Streaming/Downloading

An area of great controversy has been whether streaming implicates the reproduction right of the copyright holder at all and, if so, whether the compulsory mechanical license of Section 115 of the copyright statute applies to streaming. As discussed in Sections I.A.1 and I.A.2 above, the right of reproduction is potentially implicated when a work is streamed over the Internet because interim whole or partial copies of the work are made in various RAM memories in the course of transmission of the work. Entities that conduct streaming have sought to avoid having to pay a separate royalty under the right of reproduction based on such interim copies, in addition to a public performance royalty. In addition, controversy has arisen over what royalty rates should apply to copies made in the course of limited downloads, as opposed to full downloads.

Section 115(a) of the copyright statute provides for a compulsory license (referred to in the industry as a "mechanical license") to make copies of a nondramatic musical work as embodied in phonorecords or digital phonorecord deliveries ("DPDs"), provided that phonorecords of the musical work have been distributed to the public in the U.S. under authority of the copyright owner. Section 115(d) defines a "digital phonorecord delivery" to mean

each individual delivery of a phonorecord by digital transmission of a sound recording which results in a specifically identifiable reproduction by or for any transmission recipient of a phonorecord of that sound recording, regardless of whether the digital transmission is also a public performance of the sound recording or any nondramatic musical work embodied therein. A digital phonorecord delivery does not result from a

⁴²³⁵ Id. at 163-64.

⁴²³⁶ Id. at 150.

real-time, non-interactive subscription transmission of a sound recording where no reproduction of the sound recording or the musical work embodied therein is made from the inception of the transmission through to its receipt by the transmission recipient in order to make the sound recording audible.

The last sentence of this definition might be read to exclude streaming from the definition of DPDs, an issue which has been the subject of considerable controversy, as discussed further below.

Section 115(c)(3)(A) provides that the compulsory license includes the right to distribute “a phonorecord of a nondramatic musical work by means of a digital transmission which constitutes a digital phonorecord delivery, regardless of whether the digital transmission is also a public performance of the sound recording under section 106(6) ... or of any nondramatic musical work embodied therein under section 106(4).”

As in the case of the digital performance right with respect to sound recordings, the copyright statute provides for royalty rates for the compulsory mechanical license to be set through voluntary negotiation proceedings noticed by the Copyright Office and, if such proceedings fail to reach agreements, through CARP proceedings.⁴²³⁷ The copyright statute provides that, in setting the terms and rates for the compulsory license, the CARP “shall distinguish between (i) digital phonorecord deliveries where the reproduction or distribution of a phonorecord is incidental to the transmission which constitutes the digital phonorecord delivery [usually referred to as “incidental DPDs”], and (ii) digital phonorecord deliveries in general [usually referred to as “general DPDs”].”⁴²³⁸ Voluntary negotiation and/or CARP proceedings are generally to be repeated in each fifth calendar year after 1997.⁴²³⁹ A CARP proceeding, Docket No. 99-4 CARP DPRA, relating to DPDs was initiated and remained open for many years, but was terminated by the Copyright Office on Aug. 6, 2007 pursuant to the Royalty and Distribution Reform Act of 2004, which eliminated the CARP system and replaced it with the CRB. The Copyright Office noted that subsequent proceedings regarding the rates for Section 115 must be initiated under the new CRB system.⁴²⁴⁰

Because Congress did not define what constitutes an incidental DPD, much controversy has arisen with respect to them:

- Whether streaming constitutes a DPD at all;
- If so, whether streaming involves incidental DPDs or general DPDs;

⁴²³⁷ 17 U.S.C. § 115(c)(3)(C) & (D).

⁴²³⁸ *Id.* § 115(c)(3)(D).

⁴²³⁹ *Id.* § 115(c)(3)(F).

⁴²⁴⁰ 72 Fed. Reg. 45071, 45072 (Aug. 10, 2007).

- Whether limited downloads should be classified as incidental DPDs or general DPDs;
- Whether the interim copies generated in the course of streaming or limited downloads constitute a fair use or instead require a mechanical license;
- Whether the interim copies produced in the course of streaming and limited downloads are subject to the compulsory mechanical license of Section 115; and
- What royalties should be paid for the copies of works generated in the course of streaming and limited downloads.

The foregoing issues came to the fore with the rise of online music distribution systems, both “free” services such as Napster, Music City, Grokster, and Kazaa, as well as the various nascent subscription online music services such as Pressplay, MusicNet, Listen.com, and MP3.com. The issues have been fought in a variety of forums, as described in the next subsections.

(a) Applicability of the Section 115 Compulsory License to Streaming

Only two cases to date have addressed the issue of whether the compulsory mechanical license of Section 115 applies to streaming.

(1) *Rodgers & Hammerstein Org’n v. UMG Recordings*

In *Rodgers & Hammerstein Org’n v. UMG Recordings, Inc.*,⁴²⁴¹ a number of songwriters and music publishers brought an action for copyright infringement against the defendants, UMG Recordings, Inc. and The Farm Club Online, Inc., for copyright infringement. The Farm Club was a subsidiary of UMG that streamed recordings over the Internet. The plaintiffs alleged that such streaming was being conducted without proper licenses under the musical composition copyrights held by the plaintiffs. The defendants claimed that, if a mechanical license were required at all for streaming, they were entitled to the compulsory license under Section 115.⁴²⁴²

The court ruled that the Section 115 compulsory mechanical license did not permit the defendants to stream the copyrighted works at issue over the Internet.⁴²⁴³ The court pointed to Section 115(a)(1), which provides that a “person may obtain a compulsory license only if his or her primary purpose in making phonorecords is to distribute them to the public for private use.” The court noted that the defendants did not fall within this language because they did not sell copies of records to their users, but rather merely placed copies of recordings on their servers to

⁴²⁴¹ 60 U.S.P.Q.2d 1354 (S.D.N.Y. 2001).

⁴²⁴² *Id.* at 1355-57.

⁴²⁴³ The court also held that an existing license from the Harry Fox Agency (HFA) held by the defendants did not cover the streaming because that license was limited by its terms to a specific phonorecord number, and the HFA license did not constitute a compulsory license under Section 115. *Id.* at 1357-59.

allow users to listen to songs on those records via streaming.⁴²⁴⁴ Nor did the copies stored by the defendants on their servers trigger applicability of the compulsory mechanical license:

Thus the Defendants' server copies of the copyrighted works are not analogous to master recordings made in the course of the process of making phonorecords to be distributed to the public. Defendants concede that their server copies themselves are not for distribution to the public. Since Defendants' server copies are neither intended for distribution to the public nor part of a process for distributing digital copies of the existing phonorecords, Section 115 would not give the Defendants a right to a compulsory license for the server copies.⁴²⁴⁵

Accordingly, the court denied the defendants' motion for summary judgment that they were licensed to stream the works.⁴²⁴⁶

The court also granted the plaintiffs' cross motion for partial summary judgment. The court stated:

While Defendants have been less than candid with the Court, it is clear that what Defendants are attempting to do is to limit the payments due from them for the streaming of recordings of copyrighted works to their customers to the licensing fee that would be applicable when a radio station sends a recording over the airwaves. It is obvious that Defendants do not want to pay the Plaintiffs the license fee for a record every time one of their customers listens to recording on the Internet. However, the only license that Defendants rely on here is one that is limited to the distribution of records to the public for which there is an established fee. Defendants choice is to obtain a license for that purpose and pay the fee or cease their infringing activity.⁴²⁴⁷

It is unclear what precisely the "infringing activity" was that the court was referring to. It does not seem to be the distribution of copies, for the court found the defendants were not distributing digital copies of phonorecords (and thus Section 115 did not apply). It therefore must have been the public performance of the compositions via streaming for which the defendants required a license.

(2) ABKCO Music v. Sagan

In ABKCO Music, Inc., v. Sagan,⁴²⁴⁸ the defendants acquired a collection of live audio and audiovisual recordings of iconic songs that were recorded while being performed live in concert. The defendants reproduced the recordings principally in digital format and made them available

⁴²⁴⁴ Id. at 1360.

⁴²⁴⁵ Id. (citation omitted).

⁴²⁴⁶ Id. at 1361.

⁴²⁴⁷ Id.

⁴²⁴⁸ 2018 U.S. Dist. LEXIS 60026 (S.D.N.Y. Apr. 9, 2018).

for mass consumption through digital download and streaming services offered for a fee through their web sites. The plaintiffs, who were owners or exclusive licensees of the copyrights to approximately 200 musical compositions reflected in the recordings, claimed that the defendants' exploitation of those recordings infringed their copyrights in the musical compositions. The defendants asserted that they had obtained the proper mechanical licenses for their activities by working with various third party licensing agents that grant mechanical licenses, either directly (through the Harry Fox Agency) or pursuant to the compulsory license of Section 115 (through RightsFlow Inc. and MediaNet, Inc.). The defendants further asserted that they had fulfilled their royalty payment obligations for all the recordings at issue and that the plaintiffs had never returned or rejected their payments.⁴²⁴⁹

The plaintiffs argued that audiovisual recordings are ineligible for the Section 115 compulsory license because that license is limited to making and distributing phonorecords, which in turn are defined in Section 101 as "material objects in which sounds, *other than those accompanying a motion picture or other audiovisual work*, are fixed" (emphasis added). The defendants argued to the contrary, relying on the last sentence of the definition of phonorecords, which states: "The term 'phonorecords' includes the material object in which the sounds are first fixed." The defendants claimed that because their live concert recordings "first fixed" the sounds in those recordings as part of an audiovisual work, the resulting "material object" qualified as a phonorecord. The court rejected this argument, ruling that the second sentence of the definition could not save the defendants from the first sentence's categorical exclusion of audiovisual works, because the second sentence speaks only in terms of "*the* material object in which *the sounds* are first fixed" (emphasis added). The second sentence thus reinforces the concept that phonorecords include only sounds, and makes no mention of audiovisual works. The use of the definite article "the" to reference the concepts "material objects" and "sounds" could only be read to refer to those terms as previously defined in the first sentence – i.e., as expressly excluding audiovisual works. Accordingly, the court concluded that the Section 115 compulsory license does not cover audiovisual recordings, and the defendants' license defense therefore failed with respect to the audiovisual recordings it had made.⁴²⁵⁰

⁴²⁴⁹ Id. at *3-4, *15-16 & *30.

⁴²⁵⁰ Id. at *31-34. The court noted that its decision was consistent with a 1996 ruling of the Second Circuit, in which the Second Circuit held that the "plain language of [Section 101 of] the Copyright Act refutes" the claim that "audiovisual works" fall "within the grant of [a] compulsory license[]." Id. at *33-34 (quoting ABKCO Music, Inc. v. Stellar Records, Inc., 96 F.3d 60, 65 (2d Cir. 1996), abrogated on other grounds by Salinger v. Colting, 607 F.3d 68, 75 (2d Cir. 2010)). The court further ruled that defendants could not avail themselves of the Section 115 license because Section 115 requires that the sound recording from which the licensee is making phonorecords was lawfully fixed, and that the making of the phonorecords was authorized by the owner of copyright in the sound recording. Here, the defendants had not met their burden of establishing that their recordings were fixed or manufactured with the consent of the artists featured in them, as required by state and federal law, nor that the pre-1972 recordings were fixed pursuant to an express or valid compulsory license from the copyright holders in the musical compositions (i.e., the plaintiffs or their predecessors). ABKCO Music v. Sagan, 2018 U.S. Dist. LEXIS 60026 at *34-48.

(b) The Copyright Office's Position – The 2001 DMCA Report and Comment Proceedings

As discussed in Section II.G.6(a) above, Section 104 of the DMCA requires the Register of Copyrights and the Assistant Secretary for Communications and Information of the Commerce Department to study and report to Congress within two years of enactment of the DMCA with respect to the DMCA's impact on, among other things, "the relationship between existing and emergent technology" and Sections 109 and 117 of the copyright statute. The report required under Section 104 was issued in August of 2001 and is available online at www.loc.gov/copyright/reports/studies/dmca/dmca_study.html.

The report concluded that the making of temporary copies of a work in RAM in the course of streaming implicates the reproduction right of the copyright holder so long as the reproduction persists long enough to be perceived, copied, or communicated.⁴²⁵¹ The report noted considerable uncertainty in the industry concerning the legal status of buffer copies and the exposure of webcasters to demands for additional royalty payments from the owners of streamed sound recordings. The report expressed the belief "that there is a strong case that the making of a buffer copy in the course of streaming is a fair use," based largely on the fact that buffer copies do not supersede or supplant the market for the original works and the effect on the actual or potential market for the works appears to minimal or nonexistent.⁴²⁵² Because the sole purpose for making the buffer copies is to permit an activity that is licensed by the copyright owner and for which the copyright owner receives a performance royalty, the report concluded that copyright owners appeared "to be seeking to be paid twice for the same activity."⁴²⁵³

Accordingly, the report recommended:

that Congress enact legislation amending the Copyright Act to preclude any liability arising from the assertion of a copyright owner's reproduction right with respect to temporary buffer copies that are incidental to a licensed digital transmission of a public performance of a sound recording and any underlying musical work.

The economic value of licensed streaming is in the public performances of the musical work and the sound recording, both of which are paid for. The buffer copies have no independent economic significance. They are made solely to enable the performance of these works. The uncertainty of the present law potentially allows those who administer the reproduction right in musical works to prevent webcasting from taking place – to the detriment of other copyright owners, webcasters and consumers alike – or to extract an additional payment that is not justified by the economic value of the copies at issue. Congressional action is desirable to remove the uncertainty and to allow the activity that

⁴²⁵¹ See Section III.B.2.a of the Executive Summary of the report, which may be found online at www.loc.gov/copyright/reports/studies/dmca/dmca_executive.html.

⁴²⁵² Id. Section III.B.2.b.

⁴²⁵³ Id.

Congress sought to encourage through the adoption of the section 114 webcasting compulsory license to take place.

Although we believe that the fair use defense probably does apply to temporary buffer copies, this approach is fraught with uncertain application in the courts. This uncertainty, coupled with the apparent willingness of some copyright owners to assert claims based on the making of buffer copies, argues for statutory change.⁴²⁵⁴

On Mar. 9, 2001, prior to issuance of the 2001 DMCA report, and in response to a petition by the RIAA for rulemaking or to convene a CARP, the Copyright Office initiated a request for public comments on the interpretation and application of the mechanical and digital phonorecord compulsory license to certain digital music services, including webcasting.⁴²⁵⁵ The RIAA petition focused on two types of digital music deliveries:

– “On-Demand Stream,” defined as an “on-demand, real-time transmission using streaming technology such as Real Audio, which permits users to listen to the music they want when they want and as it is transmitted to them”; and

– “Limited Download,” defined as an “on-demand transmission of a time-limited or other use-limited (i.e. non-permanent) download to a local storage device (e.g. the hard drive of the user’s computer), using technology that causes the downloaded file to be available for listening only either during a limited time (e.g. a time certain or a time tied to ongoing subscription payments) or for a limited number of times.”⁴²⁵⁶

Music publishers had taken the position that both On-Demand Streams and Limited Downloads implicated their reproduction (mechanical license) rights. The RIAA requested the Copyright Office to determine whether On-Demand Streams are incidental DPDs and, if so, to convene a CARP to set rates for those incidental DPDs. With respect to Limited Downloads, the

⁴²⁵⁴ Id. Section III.B.2.c. The report also acknowledged a “symmetrical difficulty” faced in the online music industry relating to digital performances that are incidental to digital music downloads:

“Just as webcasters appear to be facing demands for royalty payments for incidental exercise of the reproduction right in the course of licensed public performances, it appears that companies that sell licensed digital downloads of music are facing demands for public performance royalties for a technical ‘performance’ of the underlying musical work that allegedly occurs in the course of transmitting it from the vendor’s server to the consumer’s computer.

Although we recognize that it is an unsettled point of law that is subject to debate, we do not endorse the proposition that a digital download constitutes a public performance even when no contemporaneous performance takes place. If a court were to find that such a download can be considered a public performance within the language of the Copyright Act, we believe that the arguments concerning fair use and the making of buffer copies are applicable to this performance issue as well. It is our view that no liability should result from a technical ‘performance’ that takes place in the course of a download.” Id.

⁴²⁵⁵ 66 Fed. Reg. 14099 (Mar. 9, 2001).

⁴²⁵⁶ Id. at 14100.

RIAA suggested that they may be either incidental DPDs or more in the nature of record rentals, leases or lendings.⁴²⁵⁷ In either case, the RIAA believed that the compulsory license of Section 115 should apply, but asked the Copyright Office to conduct a rulemaking proceeding with respect to the issues:

In sum, RIAA asserts that it is unclear whether the section 115 license permits all of the activities necessary to make On-Demand Streams or Limited Downloads, and if so, at what royalty rates. Consequently, RIAA petitions the Office to determine (1) whether On-Demand Streams are incidental DPDs covered by the license; (2) whether the license includes the right to make server copies or other copies necessary to transmit On-Demand Streams and Limited Downloads; and (3) the royalty rate applicable to On-Demand Streams (if they are covered by the license) and Limited Downloads.⁴²⁵⁸

The Copyright Office sought public comment on these issues and other related issues, including the following:

- “Is it possible to define ‘incidental DPD’ through a rulemaking proceeding?”⁴²⁵⁹
- “Are some or all the copies of a musical work made that are necessary to stream that work incidental DPDs?”⁴²⁶⁰
- “Aren’t incidental DPDs subject to section 115’s definition of digital phonorecord deliveries? If so, does the requirement that a DPD result in a ‘specifically identifiable reproduction’ by or for a transmission recipient rule out some of the copies discussed above from consideration as incidental or general DPDs?”⁴²⁶¹

(c) The NMPA/HFA/RIAA Agreement of 2001

While the public comment proceedings were ongoing, the RIAA and music publishers, acting through the National Music Publishers Association (NMPA) and the Harry Fox Agency (HFA), announced on Oct. 9, 2001 a breakthrough agreement on the licensing of musical works for new subscription services over the Internet. According to a joint statement filed by NMPA, HFA and RIAA with the Copyright Office on Dec. 6, 2001, the agreement applies to subscription digital music services that include among their offerings “On-Demand Streams” (defined as “an on-demand, real-time transmission of a song to a consumer who requests that song using

⁴²⁵⁷ Id.

⁴²⁵⁸ Id. at 14100-101.

⁴²⁵⁹ Id. at 14101.

⁴²⁶⁰ Id.

⁴²⁶¹ Id. at 14102.

streaming technology”) and/or “Limited Downloads” (defined as “a download that can be played for a limited period of time or a limited number of plays”).⁴²⁶²

Under the agreement, the parties agreed that a mechanical license under Section 115 for On-Demand Streams and Limited Downloads is available (contrary to the holding of the Rodgers and Hammerstein case discussed in Section III.E.4(a) above) through HFA to all RIAA member companies and to any digital music service that is majority owned by one or more RIAA members. The rights under any such license can be extended to any service authorized by a licensee to make On-Demand Streams and/or Limited Downloads of a licensed musical work. In addition, NMPA and HFA publicly announced that it is their policy to license not only RIAA members but also other digital music services that wish to negotiate comparable agreements.⁴²⁶³

The agreement provides that a mechanical license obtained under it includes all reproduction and distribution rights for delivery of On-Demand Streams and Limited Downloads. The agreement confirms that a mechanical license for these services includes the right to make server copies, buffer copies and other related copies used in the operation of the services. The license does not include performance rights, which are licensable separately through performing rights organizations such as ASCAP, BMI and SESAC.⁴²⁶⁴ The agreement does not establish specific royalty rates. The parties to the agreement committed to negotiate those rates pursuant to the procedures of Sections 115(c)(3)(B),(C), and (F) of the copyright statute (described in the opening paragraphs to Section III.E.4 above). If negotiations are not successful, the applicable rates are to be determined through CARP proceedings.⁴²⁶⁵

Finally, under the agreement the parties agreed to the following legal points: (1) that the process of making On-Demand Streams and Limited Downloads, from the making of server copies to the transmission and local storage of the stream or download, viewed in its entirety, involves the making and distribution of a DPD; (2) that a compulsory license is available under Section 115 for On-Demand Streams and Limited Downloads; and (3) radio-style and other non-interactive webcasting that would qualify for a statutory license under Section 114(d)(2) does not involve the making or distribution of a DPD and thus does not require a mechanical license.⁴²⁶⁶

On Dec. 14, 2001, the Copyright Office sought public comments on the effect of the RIAA/NMPA/HFA agreement on the issues identified in its public comment proceedings initiated

⁴²⁶² Joint Statement of The Recording Industry Association of America, Inc., National Music Publishers’ Association, Inc. and The Harry Fox Agency, Inc., *In re Matter of Mechanical and Digital Phonorecord Delivery Compulsory License*, Docket No. RM 2000-7 (Dec. 6, 2001), at 3 (available as of Feb. 9, 2002 at www.loc.gov/copyright/carp/10-5agreement.pdf).

⁴²⁶³ Id. at 3-4.

⁴²⁶⁴ Id. at 4.

⁴²⁶⁵ Id. at 5.

⁴²⁶⁶ Id. at 6.

on Mar. 9, 2001.⁴²⁶⁷ The period for comment on the RIAA/NMPA/HFA agreement was extended to Feb. 6, 2002, with reply comments due on Feb. 27, 2002.⁴²⁶⁸

On June 22, 2004, the Copyright Office amended its regulations governing the content and service of notices on the copyright owner required to take advantage of the compulsory license of Section 115. The purpose of the amended regulations was to simplify the notice process for digital music services wishing to take advantage of the compulsory license for a broad spectrum of musical works embodied in sound recordings.⁴²⁶⁹

(d) The Interactive Streaming and Limited Download Agreement of 2008

On Jan. 7, 2008, DiMA requested pursuant to Section 802(f)(1)(B) that the CRB refer to the Register of Copyrights the question of whether interactive streaming constituted a DPD. Copyright Owners objected to the request, and after holding oral arguments on the question, the CRB denied the request, stating that the question of what is “interactive streaming” is a question of fact, not a question of law as required by Section 802(f)(1)(B).⁴²⁷⁰

On September 22, 2008, a royalty agreement was announced between DiMA, the RIAA, the national Music Publishers’ Association (NMPA), the Nashville Songwriters Association International (NSAI), and the Songwriters Guild of America (SGA). The agreement proposed mechanical royalty rates for interactive streaming and limited downloads, inclusive of subscription and ad-supported services, and generally called for rates of 10.5% of revenue, minus amounts owed for performance royalties. The parties also confirmed that reproduction or distribution licenses are not required from copyright owners for non-interactive, audio-only streaming services.⁴²⁷¹ The agreement was published on Oct. 1 with a request for comments.⁴²⁷² After releasing its Initial Determination on Oct. 2, the CRB issued its Final Determination of Rates and Terms in the Matter of Mechanical and Digital Phonorecord Delivery Rate Determination Proceeding on Nov. 24, and published it on Jan. 26, 2009.⁴²⁷³

On Jan. 8, 2009 the Register solicited comments from the participants regarding potential legal errors in the CRB’s Final Determination, and received responses from the RIAA, Copyright Owners, and DiMA. Concurrent with the publication of the Final Determination on Jan. 26, the

⁴²⁶⁷ 66 Fed. Reg. 64783 (Dec. 14, 2001).

⁴²⁶⁸ 67 Fed. Reg. 4694 (Jan. 31, 2002).

⁴²⁶⁹ 69 Fed. Reg. 34578 (June 22, 2004).

⁴²⁷⁰ See 74 Fed. Reg. 4537, 4538 (Jan. 26, 2009).

⁴²⁷¹ Brendan Pierson, “Music Groups Strike Deal on Internet Royalties,” *Law360* (Sept. 24, 2008), available as of Aug. 1, 2012 at <http://www.law360.com/ip/articles/70323>; DiMA, “Major Music Industry Groups Announce Breakthrough Agreement” (Sept. 23, 2008), available as of Aug. 1, 2012 at <http://www.digmedia.org/component/content/article/40-press-releases/128-press-releases-9-23-08>.

⁴²⁷² 73 Fed. Reg. 57033 (Oct. 1, 2008).

⁴²⁷³ 74 Fed. Reg. 4510 (Jan. 26, 2009).

Register issued a decision ruling that some elements of the Final Determination were in error, and rejecting the CRB's earlier conclusion that it lacked authority to review the legality of the terms of the agreements.⁴²⁷⁴ In particular, the Register identified four erroneous provisions: (1) the definition of "interactive stream" was erroneous because it altered the provisions of the Section 115 license regarding what constitutes a DPD; (2) the promotional royalty rate for interactive streams and limited downloads constituted retroactive rulemaking; (3) the timing of royalty payments provision violated 17 U.S.C. § 115(c)(5); and (4) the Register cannot prescribe regulations on statements of account, as directed in the Final Determination.⁴²⁷⁵ In response, the CRB deleted from the Final Determination the four provisions that the Register identified, but did not add any new provisions to correct the errors.⁴²⁷⁶ In doing so, the CRB noted that although the Register's decision is binding as precedent only on subsequent proceedings, the CRB chose to exercise its ability to modify the terms (but not the rates) of an agreement, so as to avoid potential confusion for users of the license at issue.⁴²⁷⁷

(e) 2008 Interim Regulation re Compulsory DPD License

Following a notice of proposed rulemaking, the Copyright Office announced on Nov. 7, 2008 an interim regulation concerning the Section 115 mechanical license for making and distributing DPDs. Initially, the proposed rule defined a DPD as including all buffer copies made in the course of streaming, meaning that all music streaming would therefore have been included in the scope of the mechanical license. However, in light of comments and testimony, as well as uncertainties created by the Cartoon Network LP v. CSC Holdings, Inc.⁴²⁷⁸ decision, the resulting Interim Regulation backtracked. The Interim Regulation "takes no position on whether or when a buffer copy independently qualifies as a DPD, or whether or when it is necessary to obtain a license to cover the reproduction or distribution of a musical work in order to engage in activities such as streaming."⁴²⁷⁹ Instead, the Interim Regulation simply clarifies that "(1) whenever there is a transmission that results in a DPD, all reproductions made for the purpose of making the DPD are also included as part of the DPD, and (2) limited downloads qualify as DPDs."⁴²⁸⁰ As explained below, the Interim Regulation also does not define the duration threshold at which a DPD occurs for the purposes of "fixation."⁴²⁸¹

The issue of fixation vexed the Copyright Office because Cartoon Network indicated that if a reproduction was not fixed for a sufficient duration then it did not qualify as an infringement

⁴²⁷⁴ 74 Fed. Reg. 4537 (Jan. 26, 2009).

⁴²⁷⁵ Id.

⁴²⁷⁶ 74 Fed. Reg. 6832 (Feb. 11, 2009).

⁴²⁷⁷ Id. at 6833.

⁴²⁷⁸ 536 F.3d 121 (2d Cir. 2008), cert. denied sub nom. CNN, Inc. v. CSC Holdings, Inc., 557 U.S. 946 (2009).

⁴²⁷⁹ 73 Fed. Reg. 66173, 66174 (Nov. 7, 2008).

⁴²⁸⁰ Id.

⁴²⁸¹ Id.

of the right of reproduction. However, Cartoon Network provided no clear answers as to the minimum duration that still constituted fixation. After considering Cartoon Network's determination that a buffer that held a work for not more than 1.2 seconds is not “fixed,” and contrasting it with the ruling in MAI Sys. Corp. v. Peak Computer, Inc.,⁴²⁸² which held that a duration of several minutes was sufficiently fixed, the interim regulation concluded that Cartoon Network did not provide guidance as to the minimum duration sufficient for fixation.

Because of this uncertainty, the interim regulation declined to address whether streaming music that involves making buffer copies (but makes no other copies) is included in the Section 115 mechanical license.⁴²⁸³ Nonetheless, the Interim Regulation did respond to Cartoon Network by altering 37 CFR 201.18 to include the requirement that a DPD be “sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.”⁴²⁸⁴ Although the Regulation noted that some, if not many, such buffer copies constitute DPDs, it left it to the marketplace to decide the issue, noting that most licenses that are made pursuant to Section 115 are not actually mechanical licenses, but rather are voluntary licenses that mirror the rates for mechanical licenses. Providing some clarification, however, the Interim Regulation did state that cached copies on users’ hard drives that are created by streaming services do satisfy the fixation/reproduction requirement and thereby qualify as DPDs.⁴²⁸⁵ It further resolved a disagreement over who must be able to perceive a copy in order for it to be “specifically identifiable” and therefore qualify under one of the requirements for DPDs, stating that copies that are identifiable by *any* human or computer are thereby “specifically identifiable.”⁴²⁸⁶

The Interim Regulation declined to comment on what differentiates an “incidental DPD” from an ordinary DPD, noting that the distinction is not often important because both are included under the Section 115 license, and stating that if a differentiation was ever required in a particular case, it could be made in the context of a factual analysis before the CRB. The Interim Regulation did, however, state that limited downloads qualify as DPDs, citing the fact that they are delivered, they are phonorecords, and they are specifically identifiable.⁴²⁸⁷ According to the interim regulation, any copy of a phonorecord made in the process of making and distributing a DPD is covered under the Section 115 license, even if the copy is not delivered to the recipient. However, “server and intermediate copies that are the source of a transmission that does not result in the making and distribution of a DPD would not fall within the scope of the [Section 115 mechanical] license.”⁴²⁸⁸

⁴²⁸² 991 F.2d 511 (9th Cir. 1993), cert. dismissed, 114 S. Ct. 672 (1994).

⁴²⁸³ Id. at 66177.

⁴²⁸⁴ Id. at 66181.

⁴²⁸⁵ Id.

⁴²⁸⁶ Id. at 66178.

⁴²⁸⁷ Id. at 66178-79.

⁴²⁸⁸ Id. at 66180.

(f) Applicability of the Section 115 Compulsory License to Ringtones

In October of 2006, in response to a request by the Copyright Royalty Board for a ruling, the Copyright Office issued a memorandum opinion concluding that ringtones qualify as DPDs eligible for the statutory license of Section 115. Specifically, the Copyright Office ruled as follows:

We find that ringtones (including monophonic and polyphonic ringtones, as well as mastertones) are phonorecords and the delivery of such by wire or wireless technology meets the definition of DPD set forth in the Copyright Act. However, there are a variety of different types of ringtones ranging from those that are simple excerpts taken from a larger musical work to ones that include additional material and may be considered original musical works in and of themselves. Ringtones that are merely excerpts of a preexisting sound recording fall squarely within the scope of the statutory license, whereas those that contain additional material may actually be considered original derivative works and therefore outside the scope of the Section 115 license. Moreover, we decide that a ringtone is made and distributed for private use even though some consumers may purchase them for the purpose of identifying themselves in public. We also conclude that if a newly created ringtone is considered a derivative work, and the work has been first distributed with the authorization of the copyright owner, then any person may use the statutory license to make and distribute the musical work in the ringtone.⁴²⁸⁹

In Recording Industry Ass’n of America, Inc. v. Librarian of Congress,⁴²⁹⁰ the D.C. Circuit held that the Copyright Royalty Board’s imposition under the Section 115 compulsory license of a 1.5% per month late fee and a 24 cent royalty for every ring tone sold using copyrighted work were fair measures to compensate copyright owners when their work is copied absent a negotiated license agreement and were therefore not arbitrary and capricious.

(g) Subsequent Determinations of Compulsory License Rates by the CRB

After conducting rate determination proceedings in 2011-12, on Apr. 11, 2012, the CRB received a motion to adopt a settlement reached by all participants in the proceeding, and adopted the settlement pursuant to a determination published in Nov. 13, 2013 setting forth the rates and terms for the Section 115 compulsory license for the use of musical works in physical phonorecord deliveries, permanent digital downloads, ringtones, interactive streaming, limited downloads, limited offerings, mixed service bundles, music bundles, paid locker services, and purchased content locker services.⁴²⁹¹ The regulations promulgated by the CRB state (37 C.F.R. § 385.10), “Neither this subpart nor the act of obtaining a license under 17 U.S.C. 115 is intended to express or imply any conclusion as to the circumstances in which any of the exclusive rights of

⁴²⁸⁹ 71 Fed. R46350002eg. 64303, 64304 (Nov. 1, 2006).

⁴²⁹⁰ 608 F.3d 861 (D.C. Cir. 2010).

⁴²⁹¹ 78 Fed. Reg. 67938 Nov. 13, 2013).

a copyright owner are implicated or a license, including a compulsory license pursuant to 17 U.S.C. 115, must be obtained.”⁴²⁹² The regulations further state (37 C.F.R. § 385.25), “A compulsory license under 17 U.S.C. 115 extends to all reproduction and distribution rights that may be necessary for the provision of the licensed subpart C activity, as defined in § 385.21, solely for the purpose of providing such licensed subpart C activity, as defined in § 385.21 (and no other purpose).”⁴²⁹³

5. The Section 111 Compulsory License for Cable Systems

Section 111 of the Copyright Act makes available a statutory license permitting a “cable system” to publicly perform and retransmit signals of copyrighted television programming to its subscribers, provided it pays royalties at government-regulated rates and abides by the statute’s procedures. Section 111 defines a “cable system” as “a facility ... that in whole or in part [1] receives signals transmitted or programs broadcast by one or more television broadcast stations licensed by the Federal Communications Commission, and [2] makes secondary transmission of such signals or programs by wires, cables, microwave, or other communications channels to subscribing members of the public who pay for such service.” 17 U.S.C. § 111.

Most courts addressing the issue have ruled that the Section 111 statutory license is not applicable to retransmission of broadcast programming via Internet streaming.

(a) WPIX v. ivi

In WPIX, Inc. v. ivi, Inc.⁴²⁹⁴ the defendant ivi captured and retransmitted the plaintiff WPIX’s copyrighted television programming live and over the Internet to paying ivi subscribers who had downloaded ivi’s “TV player” on their computers for a monthly subscription of \$4.99. For an additional \$0.99 per month, subscribers were able to record, pause, fast-forward, and rewind ivi’s streams. In response to a lawsuit for copyright infringement, ivi claimed that it was a cable system entitled to the compulsory license under Section 111. A district court in New York rejected that argument and issued a preliminary injunction against ivi. On appeal, the Second Circuit affirmed, concluding (in accordance with the Copyright Office) that the compulsory license of Section 111 applies only to localized retransmission services regulated as cable systems by the FCC, and that Internet retransmission services are not cable systems and accordingly do not qualify for that license.⁴²⁹⁵

(b) CBS v. FilmOn

In this case, discussed in further detail in Section II.B.15 above, FilmOn argued that in light of the Supreme Court’s findings in Aereo (discussed in Section II.B.10 above), it qualified as

⁴²⁹² Id. at 67942.

⁴²⁹³ Id. at 67951.

⁴²⁹⁴ 691 F.3d 275 (2d Cir. 2012), cert. denied, 133 S. Ct. 1585 (2013).

⁴²⁹⁵ Id. at 277, 282-84.

a cable system and was entitled to the benefits and responsibility of the compulsory license scheme under Section 111 of the Copyright Act. The court rejected this, noting that the Supreme Court’s statements that Aereo (and, by extension, FilmOn, which used technology identical to Aereo) was very similar to a cable system were not the same as a judicial finding that Aereo and its technological peers are, in fact, cable companies entitled to retransmission licenses under Section 111.⁴²⁹⁶ The district court further noted that the Supreme Court’s Aereo decision did not mention, let alone abrogate, WPIX, Inc. v. ivi, Inc.,⁴²⁹⁷ which established the law in the Second Circuit that Internet retransmission services do not constitute cable systems under Section 111.⁴²⁹⁸

In May of 2017, FilmOn reached a settlement with several television broadcasters, ending its long-running fights with those broadcasters in multiple jurisdictions (further discussed in subsections III.E.5(d), (e) and (f) below) over whether Internet streaming services can utilize the Section 111 retransmission license. FilmOn’s attorney reported that FilmOn had confidentially settled appeals of the issue in cases at the D.C., Seventh and Ninth Circuits.⁴²⁹⁹

(c) American Broadcasting v. Aereo

In this case, discussed in Section II.B.10 above, a district court in New York followed the Second Circuit’s decision in WPIX, Inc. v. ivi, Inc. to conclude that Aereo’s activity of Internet retransmissions of copyrighted broadcasts was not entitled to the Section 111 compulsory license.⁴³⁰⁰

(d) Fox Television v. AereoKiller

In this case, a district court in the Central District of California disagreed with the Second Circuit’s decision in WPIX v. ivi and the Copyright Office’s position, and concluded that the defendant FilmOn (formerly known as AereoKiller and BarryDriller) could potentially qualify for a Section 111 compulsory license.⁴³⁰¹ The court reached its conclusion largely on the ground that previous cases litigating the scope of Section 111 suggest that courts have tended to leave to Congress the task of adjusting the statute in response to changing technology. The court found support in the rationale of the Supreme Court’s decision in the Aereo case – in which the Supreme Court observed that the Aereo system (which involved technology essentially the same

⁴²⁹⁶ CBS Broadcasting Inc. v. FilmOn.com, Inc., 2014 U.S. Dist. LEXIS 101894 at *11 (S.D.N.Y. July 24, 2014).

“Defendant may argue that the Supreme Court’s language in Aereo implies that FilmOn may be entitled to a license under § 111, but an implication is not a holding.” Id.

⁴²⁹⁷ 691 F.3d 275 (2d Cir. 2012), cert. denied, 133 S. Ct. 1585 (2013).

⁴²⁹⁸ FilmOn, 2014 U.S. Dist. LEXIS 101894 at *6, *11-12.

⁴²⁹⁹ Kelcee Griffis, “FilmOn Drops TV Copyright Appeals in 3 Circuits,” *Law360* (May 15, 2017), available as of May 23, 2017 at <https://www.law360.com/articles/923863>.

⁴³⁰⁰ American Broadcasting Cos. v. Aereo, Inc., 2014 U.S. Dist. LEXIS 150555 at *15-19 (S.D.N.Y. Oct. 23, 2014).

⁴³⁰¹ Fox Television Stations, Inc. v. AereoKiller, 115 F. Supp. 3d 1152 (C.D. Cal. 2015), rev’d, 851 F.3d 1002 (9th Cir. 2017).

as the present case) bore an “overwhelming likeness to the cable companies targeted by the 1976 amendments”⁴³⁰² – continued the trajectory started in Fortnightly and seen in later decisions concerning satellite technology: “courts consistently reject the argument that technological changes affect the balance of rights as between broadcasters and retransmitters in the wake of technological innovation.”⁴³⁰³

The district court found the Copyright Office’s contrary position not persuasive and the result of a policy bias, as reflected in the Copyright Office’s call for the repeal of Section 111 since 1982 and its consistent opposition to the satellite compulsory licenses. The court found that the Copyright Office’s policy views appeared to have found expression in a very strange reading of the words “facility” and “communications” in Section 111. The court therefore concluded it was questionable whether deference should be given to the Copyright Office’s interpretation of Section 111.⁴³⁰⁴

The district court also disagreed with the rationale of the Second Circuit’s WPIX v. ivi decision, which found it unclear whether ivi was a “facility” that received broadcast signals and made secondary transmissions because it was unclear whether the Internet itself is a facility, as it is neither a physical nor a tangible entity, but rather a global network of millions of interconnected computers.⁴³⁰⁵ The court found no such lack of clarity here, because the “Internet” was not the “facility” urged by the defendants. Rather, the district court found that the undisputed facts in this case were that the signals were not received by the Internet, but by antennas, located in particular buildings wholly within particular states. The signals were then retransmitted out of those facilities on “wires, cables, microwave, or other communications channels.”⁴³⁰⁶ Thus, the nebulous nature of the Internet did not bear on whether the defendants operated equipment that “receives signals transmitted or programs broadcast by one or more television broadcast stations,” reformatted those signals, and then sent them out to the viewing public.⁴³⁰⁷ The court therefore concluded that, were defendants to remedy some failings to comply with FCC broadcast regulations, they would be entitled to a Section 111 license.⁴³⁰⁸ The court, however, considered the question to be “close” and therefore authorized an immediate appeal to the Ninth Circuit pursuant to Fed. R. Civ. P. 54(b) and stayed further proceedings pending such appeal.⁴³⁰⁹

⁴³⁰² American Broadcasting Co. v. Aereo, Inc., 134 S. Ct. 2498, 2504 (2014).

⁴³⁰³ AereoKiller, 115 F. Supp. 3d at 1163.

⁴³⁰⁴ Id. at 1164-66.

⁴³⁰⁵ Id. at 1166-67 (citing WPIX, Inc. v. ivi, 691 F.3d 275, 280-82 (2d Cir. 2012), cert. denied, 133 S. Ct. 1585 (2013)).

⁴³⁰⁶ AereoKiller, 115 F. Supp. 3d at 1167-68.

⁴³⁰⁷ Id. at 1167.

⁴³⁰⁸ Id. at 1171.

⁴³⁰⁹ Id.

On appeal, the Ninth Circuit reversed.⁴³¹⁰ As an initial matter, the court rejected Fox’s very stringent interpretation of the definition of “cable system” in Section 111(f)(3), which is a “facility” that “in whole or in part receives signals transmitted or programs broadcast by one or more television broadcast stations licensed by the Federal Communications Commission, and makes secondary transmissions of such signals or programs by wires, cables, microwave, or other communications channels to subscribing members of the public who pay for such service.”⁴³¹¹ Fox argued that the relevant “facility” must comprise both a retransmission service’s means of receiving broadcast signals *and* its means of making secondary transmissions to paying subscribers. Under Fox’s reading, FilmOn would be excluded from the definition of “cable system” because it retransmitted broadcast signals over the Internet, a facility that was not under its ownership or control. The court rejected this reading, finding that nothing in the definition on its face compelled the conclusion that the facility must *control* the retransmission medium (the wires, cables, microwaves or other communications channels) that it relied on to deliver the retransmissions. The court also noted that the Copyright Office had not endorsed Fox’s reading.⁴³¹²

The court also rejected FilmOn’s position that Section 111 makes compulsory licenses available to any facility that retransmits broadcast signals or programming, no matter its technological features or characteristics. The court noted that Congress had limited the Section 111 licenses to only specific technologies recited in the definition, and had provided separate compulsory license provisions in §§ 119 and 122 for broadcast retransmissions by satellite carriers. The court also found it far from clear whether, as FilmOn argued, the Internet should count as one of the “other communications channels” envisioned by Section 111. The court noted Fox’s expert argued that the defining characteristics of a communications channel in electrical engineering terms are bandwidth, noise and throughput, and under that definition the Internet is not a communications channel. The court also noted that under the *ejusdem generis* canon of statutory construction, one could reasonably conclude that the “other communications channels” referenced in the definition must share characteristics such as bandwidth, throughput and noise. Alternatively, one could conclude, as the Copyright Office had, that such channels must be inherently localized transmission media of limited availability.⁴³¹³

From a policy perspective, the court noted that Section 111 was Congress’ attempt to balance the socially useful role cable systems had come to play, on the one hand, against the property interests and creative incentives of copyright holders, on the other, and one could argue that Internet-based retransmission systems might pose a more serious threat to the value and integrity of copyrighted works than traditional cable systems. The array of competing interests at stake therefore did not unambiguously counsel for or against a broad reading of Section 111. Finally, the court found the legislative history to be a “wash,” neither compelling

⁴³¹⁰ Fox Televisions Stations, Inc. v. Aereokiller, LLC, 851 F.3d 1002 (9th Cir. 2017).

⁴³¹¹ 17 U.S.C. § 111(f)(3).

⁴³¹² Fox v. Aereokiller, 851 F.3d at 1008.

⁴³¹³ Id. at 1009-10.

the conclusions that Section 111 must be interpreted to be technology agnostic, or that Internet-based retransmission services must be deemed cable systems.⁴³¹⁴

The court thus concluded that the language of Section 111 is ambiguous as to whether Internet-based retransmission systems satisfy the definition of “cable system.” It therefore turned to the question of how much weight it should give to the Copyright Office’s views on the issue, noting that since 1997, the Copyright Office had on at least four occasions specifically and unequivocally stated that, in its view, Internet-based retransmission services are not “cable systems” under Section 111, although it had not done so in connection with any rulemaking. Instead, the Copyright Office had communicated its position largely through official reports and testimony before Congress.⁴³¹⁵

The court first turned to the question of whether it should afford the Copyright Office’s position the more permissive level of deference under Chevron⁴³¹⁶ or the use the less deferential framework under Skidmore,⁴³¹⁷ and decided that it would reach the same conclusion under either level of deference. Accordingly, the court proceeded under the Skidmore framework, under which the weight given to an agency interpretation depends upon the thoroughness evident in its consideration, the validity of its reasoning, its consistency with earlier and later pronouncements, and all those factors which give it power to persuade, if lacking power to control. Under that framework, the court found the Copyright Office’s decision to reject Internet-based retransmission services as not eligible for the Section 111 license because they do not use a localized retransmission medium, to have sufficient support in the text, structure, and basic purposes of the Copyright Act.⁴³¹⁸

The court therefore concluded as follows: “FilmOn and other Internet-based retransmission services are neither clearly eligible nor clearly ineligible for the compulsory license § 111 makes available to ‘cable systems.’ The Copyright Office says they are not eligible. Because the Office’s views are persuasive, and because they are reasonable, we defer to them. The judgment of the district court is therefore REVERSED.”⁴³¹⁹

In May of 2017, FilmOn reached a settlement with several television broadcasters, ending its long-running fights with those broadcasters in multiple jurisdictions over whether Internet streaming services can utilize the Section 111 retransmission license. FilmOn’s attorney

⁴³¹⁴ Id. at 1010-11.

⁴³¹⁵ Id. at 1011-12.

⁴³¹⁶ Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837 (1984).

⁴³¹⁷ Skidmore v. Swift & Co., 323 U.S. 134 (1944).

⁴³¹⁸ Fox v. Aereokiller, 851 F.3d at 1012-13.

⁴³¹⁹ Id. at 1015.

reported that FilmOn had confidentially settled appeals of the issue in cases at the D.C., Seventh and Ninth Circuits.⁴³²⁰

(e) Fox Television v. FilmOn X

In this case, a district court in the District of Columbia disagreed with the rationale of the AereoKiller decision and concluded that FilmOn X was not entitled to the Section 111 compulsory license. FilmOn X had modified its service in an effort to bring itself into compliance with Section 111 requirements. The modifications would permit its users to watch broadcast programs only if they purchased local channel subscription packages, which would be limited to those television channels available in a designated market area. FilmOn X developed a geolocation system to deny access to broadcast programming unless the viewer's digital device was located within the original broadcast's market area at the time of the retransmission.⁴³²¹

Nevertheless, the court concluded that FilmOn X was not entitled to the Section 111 license because it did not retransmit to its subscribers directly through facilities it controlled. Unlike cable companies, FilmOn X had no "headend" control center from which it both received broadcast signals and directly retransmitted them by coaxial cable, wires, or microwave links to their subscribers. Instead, FilmOn X's services retransmitted the signals to Internet service providers, as opposed to sending them directly to the subscribers' digital devices. The subscribers' devices therefore received the retransmissions, not from the "facility," but from interconnected computers through cyberspace.⁴³²² The court recognized that the physical layer through which the Internet can deliver video content may include cables, wires and microwaves. But the Internet does not deliver video content exclusively through those means, but also relies on multiple other types of distribution media, such as satellite, cellular networks and WiFi. The court observed that since satellite providers are not cable systems, it is unlikely that Congress intended for any entity that happens to employ wires and cables as a mere part of its transmission path to qualify as a cable system.⁴³²³

The court also determined that the Copyright Office's position of over fifteen years that Internet-based retransmission services are not cable systems and do not fall within Section 111 was entitled to deference. The court observed that as recently as 2014, four years after the district court's decision and two years after the Second Circuit's decision in the WPIX v. ivi case, Congress had amended the Copyright Act without rejecting or altering the Copyright office's interpretation. Accordingly, the court deferred to the Copyright Office's interpretation as an additional reason to conclude that FilmOn X was not entitled to the Section 111 license.⁴³²⁴

⁴³²⁰ Kelcee Griffis, "FilmOn Drops TV Copyright Appeals in 3 Circuits," *Law360* (May 15, 2017), available as of May 23, 2017 at <https://www.law360.com/articles/923863>.

⁴³²¹ Fox Television Stations, Inc. v. FilmOn X LLC, 150 F. Supp. 3d 1, 10-11 (D.D.C. 2015).

⁴³²² *Id.* at 19.

⁴³²³ *Id.* at 20-21.

⁴³²⁴ *Id.* at 24-29.

In May of 2017, FilmOn reached a settlement with several television broadcasters, ending its long-running fights with those broadcasters in multiple jurisdictions over whether Internet streaming services can utilize the Section 111 retransmission license. FilmOn’s attorney reported that FilmOn had confidentially settled appeals of the issue in cases at the D.C., Seventh and Ninth Circuits.⁴³²⁵

(f) FilmOn X v. Window to the World Communications

In this case, a district court in the Northern District of Illinois adopted a very similar rationale as the District of Columbia court in Fox Television v. FilmOn X to reach the conclusion that FilmOn X was not entitled to the Section 111 license. The parties disputed whether the Internet retransmissions conducted by FilmOn X were made via “other communications channels” within the second clause of the definition of “cable system” in Section 111. FilmOn X argued that whether the Internet is itself a communications channel was of no moment because when data is transmitted over the Internet, that data travels over one or more communications channels to reach its ultimate destination. The court disagreed, noting that Section 111’s definition of a “cable system” is not satisfied simply by data traveling over any communications channel at any point before its ultimate destination. Rather, the definition requires the same “facility” that “receives” the signals to make secondary transmission of such signals by wires, cables, microwave, or other communications channels to subscribing members of the public.⁴³²⁶

The court agreed with the District of Columbia court’s conclusion that the “facility” FilmOn X had control over and operated made secondary transmissions to the Internet or Internet service providers, as opposed to sending them directly to the subscribers’ digital devices. Correspondingly, the subscribers’ devices received the retransmissions, not from the “facility,” but from interconnected computers through cyberspace. The court therefore concurred with the District of Columbia court in concluding that such an Internet-based system failed to encompass the distribution medium through which signals were retransmitted directly to subscribers and therefore did not qualify as a “cable system” as defined in Section 111.⁴³²⁷

The court found further support for its conclusion in both the legislative history of Section 111 and in the Copyright Office’s longstanding interpretation that the compulsory license of Section 111 does not encompass Internet-based retransmissions. The court also found that FilmOn X’s newly added geolocation technology designed to limit retransmissions of broadcast programming to a given designated market area did not change the result. The court held that such technology did nothing to narrow the chasm between Internet retransmission services and the cable systems of Section 111. And the fact that an Internet retransmitter might voluntarily limit its services to certain geographic areas did not change the fact that Internet retransmissions

⁴³²⁵ Kelcee Griffis, “FilmOn Drops TV Copyright Appeals in 3 Circuits,” *Law360* (May 15, 2017), available as of May 23, 2017 at <https://www.law360.com/articles/923863>.

⁴³²⁶ FilmOn X, LLC v. Window to the World Communications, Inc., 2016 U.S. Dist. LEXIS 37551 at *14-16 (N.D. Ill. Mar. 23, 2015).

⁴³²⁷ *Id.* at *21.

are still capable of reaching much farther afield than the localized cable systems that Congress intended Section 111 to cover. Accordingly, the court ruled that Window to the World Communications was entitled to partial summary judgment that FilmOn X was not eligible for the Section 111 compulsory license.⁴³²⁸

In May of 2017, FilmOn reached a settlement with several television broadcasters, ending its long-running fights with those broadcasters in multiple jurisdictions over whether Internet streaming services can utilize the Section 111 retransmission license. FilmOn's attorney reported that FilmOn had confidentially settled appeals of the issue in cases at the D.C., Seventh and Ninth Circuits.⁴³²⁹

6. International Licensing Efforts

In November of 2003, the International Federation of the Phonographic Industry (IFPI), a global trade body representing major and independent music labels, announced a "one-stop" international license for webcasters. IFPI expected collection agencies in 30 to 40 countries to sign up to the single license agreement by the end of 2003. Webcasters would pay a national body a fee for songs broadcast into each individual country. The agreement would be for radio-style broadcasts only. Internet companies would still need to secure individual licensing agreements to sell permanent song downloads.⁴³³⁰

F. First Sales in Electronic Commerce

The "first sale doctrine" of copyright law is codified in Section 109 of the copyright statute. That section provides, "Notwithstanding the provisions of section 106 (3) [the exclusive distribution right], the owner of a particular copy or phonorecord lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy or phonorecord."⁴³³¹ The applicability of the first sale doctrine to "sales" through online commerce is uncertain.

Section 109 pertains to the sale or disposal of "the possession of [a] copy or phonorecord." The statute was, of course, originally drafted with tangible copies in mind. An immediate issue concerns whether an initial "sale" accomplished by an online *transmission*, rather than the physical distribution of a material object, constitutes a sale of a "copy" that would trigger the application of the doctrine at all. At least one commentator has argued that it

⁴³²⁸ *Id.* at *32-43.

⁴³²⁹ Kelcee Griffis, "FilmOn Drops TV Copyright Appeals in 3 Circuits," *Law360* (May 15, 2017), available as of May 23, 2017 at <https://www.law360.com/articles/923863>.

⁴³³⁰ "Music Industry Trumpets Global Webcast License" (Nov. 11, 2003), available as of Nov. 11, 2003 at <http://uk.news.yahoo.com/031111/80/edmp0.html>.

⁴³³¹ 17 U.S.C. § 109(a).

does not,⁴³³² and the NII White Paper notes that the issue is uncertain.⁴³³³ However, it seems plausible to analogize a transmission in which a complete authorized copy of a work ends up in permanent storage at the recipient's site (i.e., other than a transitory copy in RAM) as the distribution of a "copy" for purposes of the first sale doctrine, at least where it was intended that the recipient "own" the received copy.⁴³³⁴ Such a transaction seems highly analogous to a traditional sale of a copy, except for the distribution vehicle.

One could readily argue that in such instances the first sale doctrine should apply by analogy to permit a purchaser to further transmit his or her copy to a third party, so long as the purchaser deletes his or her original copy from storage, because in that instance, as in the case of traditional distributions of physical copies, no more total "copies" end up in circulation than were originally sold by or under authority of the copyright owner. As one commentator has noted:

[The first sale doctrine's] balance was gauged over the years Neither the copyright owner nor the copy owner receives all that it might desire. The balance could be recut today for cyberspace, but no clear reasons exist to do so. Absent that, this balance governs treatment of digital works, whether on the Internet or a diskette. Applying it is relatively simple. A purchaser who acquires a digital product that is not subject to a license has a right to retransfer the copy, make copies essential to use the work, and otherwise act as owner of the copy. If the "copy" is transferred, the transferor must relinquish all copies it possesses. Otherwise, it would in effect be making multiple copies inconsistent with the balance between copy and copyright owners.⁴³³⁵

Although this argument makes sense in many instances, such as where a buyer has purchased a copy of a book that is delivered electronically, in other instances the policy choices with respect to whether the first sale doctrine should be applied by analogy seem less clear. One such example comprises works that are made available for on-demand usage, such as movies. The copyright owner clearly intends to make such works available only for one time use by the recipient, and any further retransmission or distribution of the work to third parties would cut into the owner's on-demand market for the work. Yet depending upon the transmission technology used, a "copy" of the work may be made in whole or in part at the recipient's end. Indeed, under the MAI case, even the data stored in RAM at the recipient's computer would constitute a "copy." It seems less clear that such "copy" should trigger the first sale doctrine and permit the recipient to further distribute that "copy," even if the recipient does not retain a copy.

⁴³³² K. Stuckey, Internet and Online Law § 6.08[3][b], at 6-54 (2013).

⁴³³³ NII White Paper at 43-44.

⁴³³⁴ In the case of computer programs, copyright owners often distribute copies of the program subject to a license agreement which states that the copy is being licensed, not sold, to the user as a vehicle to avoid the applicability of the first sale doctrine to the transaction.

⁴³³⁵ R. Nimmer, Information Law ¶ 4.08[2][b], at 4-32 to 4-33 (2001).

As currently codified in Section 109, the first sale doctrine is drafted as an exception to the *distribution* right of the copyright holder. However, as discussed earlier, the new rights of transmission and access under the WIPO treaties are seemingly broader than the current distribution right under United States law. An issue therefore arises as to whether the first sale doctrine should prevail over these new rights of transmission and access, in addition to the right of distribution. Both WIPO treaties contain provisions stating that nothing in them shall affect the freedom of Contracting Parties to determine the conditions, if any, under which the exhaustion of rights afforded by the treaties will apply after the first sale or other transfer of ownership of the original or a copy of a work with the authorization of the owner.⁴³³⁶ The WIPO treaties thus seem to contemplate that the interplay between the doctrine of first sale and the new rights of transmission and access will ultimately be resolved through implementing legislation.

Although the implementing legislation in the United States afforded Congress the opportunity to resolve the ambiguities in the scope of the first sale doctrine as applied to the Internet, the DMCA does not address the issue. One of the proposed bills to implement the WIPO treaties, H.R. 3048, would have added the following new subsection (f) to Section 109 of the copyright statute with respect to applicability of the first sale doctrine to works in digital format:

(f) The authorization for use set forth in subsection (a) applies where the owner of a particular copy or phonorecord in a digital format lawfully made under this title, or any person authorized by such owner, performs, displays or distributes the work by means of transmission to a single recipient, if that person erases or destroys his or her copy or phonorecord at substantially the same time. The reproduction of the work, to the extent necessary for such performance, display, distribution, is not an infringement.

This provision seems to have been drafted to apply to the paradigm situation, discussed above, in which the original sale of a work via transmission in digital format results in a complete copy of the work residing in permanent storage at the purchaser's site. So long as the original purchaser erases his or her copy at substantially the same time, new subsection (f) permits the purchaser to transmit that copy to a third party without liability (including any reproductions, displays or performances that are attendant thereto).

The applicability of this provision to the case of on-demand transmissions for simultaneous viewing or other usage by the original purchaser (such as movies or online games) is not clear. In those instances, as discussed above, it is unclear whether the purchaser should be treated as the "owner of a particular copy or phonorecord in a digital format" by virtue of the initial on-demand download of the work in order to trigger application of the new subsection (f). In any event, this provision was not adopted in the DMCA.

⁴³³⁶ See Article 6(2) of the WIPO Copyright Treaty and Articles 8(2) and 12(2) of the WIPO Performances and Phonograms Treaty.

The European Copyright Directive appears to take the position that obtaining a copy of a copyrighted work through an online service does not exhaust the copyright owner's rights in a way that would allow resale or retransmission of such copy. Specifically, paragraph 29 of the recitals to the Directive states the following:

"The question of exhaustion does not arise in the case of services and on-line services in particular. This also applies with regard to a material copy of a work or other subject-matter made by a user of such a service with the consent of the rightholder. Therefore, the same applies to rental and lending of the original and copies of works or other subject-matter which are services by nature. Unlike CD-ROM or CD-I, where the intellectual property is incorporated in a material medium, namely an item of goods, every on-line service is in fact an act which should be subject to authorization where the copyright or related right so provides."

1. Capitol Records v. ReDigi

The District Court's Decision

In Capital Records, LLC v. ReDigi, Inc.,⁴³³⁷ ReDigi operated a web site that enabled users to "resell" their legally acquired iTunes music files and purchase "used" iTunes files from others at a fraction of the price on iTunes. To sell music on ReDigi's web site, a user was required to download ReDigi's "Media Manager" to his or her computer. Once installed, Media Manager analyzed the user's computer to build a list of digital music files eligible for sale. A file was eligible only if it was purchased on iTunes or from another ReDigi user; music downloaded from a CD or other file-sharing webs site was ineligible for sale. After the validation process, Media Manager continually ran on the user's computer and attached devices to ensure that the user had not retained music that had been sold or uploaded for sale. However, Media Manager could not detect copies stored in other locations. If a copy was detected, Media Manager prompted the user to delete the file. The file was not deleted automatically or involuntarily, although ReDigi's policy was to suspend the accounts of users who refused to comply.⁴³³⁸

Once uploaded, a digital music file underwent a second analysis to verify eligibility. If ReDigi determined that the file had not been tampered with or offered for sale by another user, the file was stored in ReDigi's "Cloud Locker," and the user was given the option of simply storing and streaming the file for personal use or offering it for sale in ReDigi's marketplace. If a user chose to sell a digital music file, the user's access to the file was terminated and transferred to the new owner at the time of purchase. When users purchased a file (at 59 cents to 79 cents), the seller received 20%, 20% went to an escrow fund for the artist, and 60% was retained by

⁴³³⁷ 934 F. Supp. 2d 640 (S.D.N.Y. 2013), aff'd, 910 F.3d 649 (2d Cir. 2018), cert. denied, 2019 U.S. LEXIS 4296 (June 24, 2019).

⁴³³⁸ Id. at 645.

ReDigi. Capitol Records sued ReDigi for direct, contributory and vicarious copyright infringement.⁴³³⁹

For the reasons discussed in Section II.A.4(v) above, the court held ReDigi liable under all three theories. The court also rejected ReDigi's assertion that the first sale doctrine permitted users to resell their digital music files on ReDigi's web site. The court noted as an initial matter that, because it had concluded that ReDigi's service violated Capitol Records' reproduction right, the first sale defense (which is a defense to a violation of the distribution right) could not apply to ReDigi's infringement of those rights. In addition, the first sale doctrine did not protect ReDigi's distribution of Capitol Records' copyrighted works because, as an unlawful reproduction, a digital music file sold on ReDigi is not "lawfully made" as required by 17 U.S.C. § 109(a). Moreover, Section 109(a) protects only distribution by the owner of a particular copy or phonorecord, and ReDigi users were not reselling the particular copies of music files they had purchased on iTunes – rather, they were producing new copies of the files on the ReDigi server. Because it was impossible for a ReDigi user to sell his or her "particular" music file on ReDigi, the first sale doctrine could not apply.⁴³⁴⁰ "Put another way, the first sale defense is limited to material items, like records, that the copyright owner put into the stream of commerce."⁴³⁴¹

The Second Circuit's Decision

On appeal, the Second Circuit affirmed.⁴³⁴² The court began by explaining in a bit of additional detail ReDigi's technology for data migration of a file from an original purchaser's computer to ReDigi's remote server known as the "Cloud Locker." ReDigi software broke the digital music file into small blocks of data of roughly four thousand bytes in length. ReDigi's system created a transitory copy of each packet in the initial purchaser's computer buffer. Upon copying or "reading" a packet into the initial purchaser's computer buffer, ReDigi's software sent a command to delete that packet of the digital file from permanent storage on the initial purchaser's device. During the data migration process, the digital file could not be accessed, played, or perceived. If connectivity was disrupted during the data migration process, the remnants of the digital file on the user's device was unusable and the transfer could not be reinitiated. In that circumstance, ReDigi bore the cost of the user's loss.⁴³⁴³

The court cast the primary issue on appeal as whether ReDigi's system lawfully enabled resales of its users' digital files. Sections 106(1) and (3) grant the copyright owner the exclusive

⁴³³⁹ Id. at 646.

⁴³⁴⁰ Id. at 655-56.

⁴³⁴¹ Id. at 655. The court also noted that, in its report on the DMCA, the U.S. Copyright Office rejected extension of the first sale doctrine to the distribution of digital works, noting that the justification for the first sale doctrine in the physical world could not be imported into the digital domain. U.S. Copyright Office, Library of Congress, DMCA Section 104 Report (2001).

⁴³⁴² Capitol Records, LLC v. ReDigi Inc., 910 F.3d 649 (2d Cir. 2018), cert. denied, 2019 U.S. LEXIS 4296 (June 24, 2019).

⁴³⁴³ Id. at 653.

right to control the reproduction and distribution of the copyrighted work. Under the first sale doctrine, codified in Section 109(a), the copyright owner's control over the *distribution* of any particular copy or phonorecord that was lawfully made effectively terminates when that copy or phonorecord is distributed to its first recipient. The court noted, however, that Section 109(a) says nothing about the copyright holder's control under Section 106(1) over *reproduction* of a copy or phonorecord. ReDigi argued on appeal that its system effectuated transfers of the *particular* digital file that the user lawfully purchased from iTunes, that it should not be deemed to have reproduced that file, and that it should therefore come within the protection of Section 109(a).⁴³⁴⁴

ReDigi offered two contentions in support of its arguments, both of which the Second Circuit rejected. First, ReDigi argued that the digital files should be considered "material objects" and therefore, under Section 101's definition of "phonorecords" as "material objects," should qualify as "phonorecords" eligible for the protection of Section 109(a). The Second Circuit ruled that it need not decide whether the digital files ReDigi transferred were phonorecords protected by Section 109(a) because the court found that ReDigi effectuated an unlawful reproduction even if the digital file itself qualified as a phonorecord.⁴³⁴⁵

Second, ReDigi argued that from a technical standpoint, its process should not be seen as making a reproduction because its system simultaneously caused packets to be removed from the file remaining in the consumer's computer as those packets were copied into the computer buffer and then transferred to the ReDigi server. Thus, the complete file never existed in more than one place at the same time, and the file on the user's machine continually shrank in size while the file on the server grew in size. As a result, the sum of the size of the data stored in the original purchaser's computer and in ReDigi's server never exceeded the size of the original file, which, according to ReDigi, confirmed that no reproductions were made during the transfer process.⁴³⁴⁶

The Second Circuit rejected this argument, pointing to the definition of phonorecords under Section 101 as material objects in which sounds are fixed by any method now known or later developed, and from which the sounds can be perceived, reproduced, or otherwise communicated, directly or with the aid of a machine or device. Accordingly, when the purchaser of a digital music file from iTunes possessed that file, embodied for a period of more than transitory duration in a computer or other physical storage device, "that device – or at least the portion of it in which the digital music file is fixed (e.g., the location on the hard drive) – becomes a phonorecord."⁴³⁴⁷ The court noted that in the course of transferring a digital music file from an original purchaser's computer, through ReDigi, to a new purchaser, the digital file was first

⁴³⁴⁴ *Id.* at 655-56.

⁴³⁴⁵ *Id.* at 656.

⁴³⁴⁶ *Id.*

⁴³⁴⁷ *Id.* at 657 (citing *London-Sire Records, Inc. v. Doe*, 542 F. Supp. 2d 153, 171 (D. Mass. 2008) (holding that the segment of a hard disc on which an electronic music file is encoded is a "phonorecord" under the Copyright Act)).

received and stored on ReDigi's server and then, at the new purchaser's option, might also be subsequently received and stored on the new purchaser's device. At each of these steps, the digital file was fixed in a new material object for a period of more than transitory duration. Accordingly, the fixing of the digital file in ReDigi's server, as well as in the new purchaser's device, created a new phonorecord, which is a reproduction. ReDigi's process for enabling the resale of digital files thus inevitably involved the creation of new phonorecords by reproduction, even if the standalone digital file was deemed to be a phonorecord.⁴³⁴⁸

As for ReDigi's reliance on the fact that as it copied a packet of data, it deleted the equivalent packet in the user's device so that the amount of data extant in the transfer process remained constant, the court ruled that this did not rebut or nullify the fact that the eventual receipt and storage of that file in ReDigi's server, as well as optionally in the new purchaser's device, did involve the making of new phonorecords. The court also ruled that it did not matter that during a transfer through ReDigi's data migration technology, each packet of data from the original source file resided in a buffer for less than a second before being overwritten because, even if the time in a computer buffer were a period of no more than transitory duration, those files subsequently became embodied in ReDigi's server and in the new purchaser's device, where they remained for periods of more than transitory duration.⁴³⁴⁹

The court further rejected ReDigi's argument, citing ABKCO Music, Inc. v. Stellar Records, Inc.,⁴³⁵⁰ that the computer hard drive into which the original purchaser's digital file was embedded could not be her lawfully made phonorecord. ReDigi argued that a computer hard drive cannot qualify as a phonorecord under Section 101 because it contains more than a sound recording. The court ruled that the argument misinterpreted ABKO, which held that a license to publish a phonorecord did not authorize the publication of compact discs for use in karaoke that contained both sound recordings and visual depictions of song lyrics. The court noted that the ABKO opinion was directed at construing the breadth of a compulsory license and does not support the conclusion that a compact disc that stores visual depictions of words as well as recorded music does not *contain* a phonorecord. In sum, the court concluded that operation of ReDigi's system resulted in the making of at least one unauthorized reproduction, and an unauthorized reproduction is not protected by Section 109(a).⁴³⁵¹

⁴³⁴⁸ ReDigi, 910 F.3d at 657.

⁴³⁴⁹ Id. at 657-58. The court also noted that even if offsetting deletions of original copies held by the transferring consumer were made, ReDigi's process still involved the making of unauthorized reproductions that infringed the exclusive reproduction right unless justified by fair use. Id. at 658.

⁴³⁵⁰ 96 F.3d 60 (2d Cir. 1996).

⁴³⁵¹ ReDigi, 910 F.3d at 658-59. The also rejected ReDigi's reliance on the Ninth Circuit's decision in Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., 180 F.3d 1072 (9th Cir. 1999). In Diamond, the Ninth Circuit held that a hard drive is excluded from the definition of a "digital musical recording" under the AHRA because Section 1001(5)(B) expressly provides that a "digital musical recording" does not include material objects "in which one or more computer programs are fixed," and "a hard drive is a material object in which one or more [computer] programs are fixed." Id. at 1076. The Second Circuit held that even if it were to accept the Ninth

The court then affirmed the district court's finding that ReDigi's actions were not protected under the doctrine of fair use. As did the district court, the Second Circuit relied principally on the first and fourth fair use factors. As to the first factor, the court noted that ReDigi made no change in the copyrighted work, and its resales of those works competed with sales of the same recorded music by the rights holder. ReDigi was hosting a remunerative marketplace that enabled resale by purchasers of digital music files, which is a commercial purpose. Especially in view of the total absence (or at least very low degree) of transformative purpose, the commercial motivation here cut against ReDigi with respect to the first factor.⁴³⁵²

With respect to the fourth factor, the court noted that ReDigi was making reproductions of the plaintiffs' works for the purpose of resale in competition with the plaintiffs' market for the sale of their sound recordings, although the court noted in dicta in a footnote that to the extent a reproduction was made solely for cloud storage of the user's music on ReDigi's server, and not to facilitate resale, the reproduction would likely be fair use just as the copying at issue in Sony was fair use.⁴³⁵³ ReDigi's copies were sold to the same consumers whose objective in purchasing was to acquire the plaintiffs' music. And the court noted a distinction between ReDigi's resales and resales of physical books and records, in that the digital files resold by ReDigi, although used, do not deteriorate the way printed books and physical records do. The fourth factor therefore weighed powerfully against fair use, and the court found, in weighing all four factors, that ReDigi had no fair use justification for its copying.⁴³⁵⁴

G. Pop-Up Advertising

1. The Gator Litigations

In June of 2002, a number of publishing companies and other entities operating their own web sites sued Gator Corporation for copyright infringement, trademark infringement, unfair competition and other causes of action based on Gator's causing unauthorized pop-up advertising to appear on the sites of the plaintiffs. Gator widely distributed a software application called "Gator" that acted as a digital wallet to provide users with a mechanism for storing personal information about themselves, passwords, user identification numbers and names and other data that consumers routinely need to input on electronic forms when shopping on the Internet. Gator bundled with the digital wallet software another program called "OfferCompanion," which, once installed, would automatically launch whenever a user initiated a browser-based Internet connection, observe the sites visited by the user, and whenever the

Circuit's construction of the term "digital musical recording" under the AHRA, that would not alter the meaning of the term "phonorecord" under Section 101 of the Copyright Act. ReDigi, 910 F.3d at 659 n.13.

⁴³⁵² Id. at 661.

⁴³⁵³ Id. at 662 & n. 16.

⁴³⁵⁴ Id. at 662-63.

user visited certain websites, display one or more unauthorized pop-up advertisements directly over such websites, obscuring a portion of the content of the website.⁴³⁵⁵

Gator sold its pop-up advertising services to various clients, who in many instances would engage the Gator service to cause the clients' pop-up ads to appear when users visited competitor's sites. For example, a Gator pop-up advertisement for hotjobs.com would appear on the home page of the plaintiff Dow Jones' CareerJournal.com web site, a classified recruitment advertising site that competed with hotjobs.com.⁴³⁵⁶ The plaintiffs sought a preliminary injunction against Gator on the grounds, among others, that the unauthorized display of Gator ads on the plaintiffs' sites infringed the plaintiffs' exclusive right of distribution under copyright law and constituted the making of unauthorized derivative works.

With respect to the distribution right, the plaintiffs argued that each of their web sites were governed by a "terms and conditions of use" that granted site visitors a license to use and display the copyrighted content of the site but not to alter the site or change its appearance. Because Gator's pop-up advertising altered the appearance of the plaintiffs' web sites by covering a portion of the content of the web page on which the ads appeared, the ads caused the site visitors to generate an infringing altered display of the web sites, and Gator was secondarily liable for contributing to such infringing displays.⁴³⁵⁷ The plaintiffs further argued that the altered displays constituted the creation of unauthorized derivative works for which Gator was directly liable.⁴³⁵⁸

On July 16, 2002, the district court entered a preliminary injunction, without written opinion, enjoining Gator from causing its pop-up advertisements to be displayed on any web site owned by or affiliated with the plaintiffs without their express consent, and from altering or modifying, or causing any other entity to alter or modify, any part of such websites or the display

⁴³⁵⁵ Memorandum in Support of Plaintiffs' Motion for Preliminary Injunction, Washingtonpost.Newsweek Interactive Co. v. The Gator Corporation, Civil Action 02-909-A (E.D. Va. June 25, 2002), at 8-10 (copy on file with the author).

⁴³⁵⁶ Id. at 10.

⁴³⁵⁷ Id. at 23-25.

⁴³⁵⁸ Id. at 25-26. The plaintiffs also argued that Gator's activities constituted trademark infringement because the plaintiffs' trademarks were clearly visible beside Gator pop-up advertisements, creating an unauthorized association between the two, and because of a likelihood of confusion as to sponsorship of the ads. The plaintiffs submitted a consumer survey in which 66% of respondents stated they believed that pop-up advertisements are sponsored by or authorized by the web site in which they appear, and 45% believed that pop-up advertisements have been pre-screened and approved by the web site on which they appear. Id. at 19-21.

thereof.⁴³⁵⁹ In February of 2003, Gator reached a settlement with 16 publishers, the terms of which were confidential.⁴³⁶⁰

A number of other lawsuits against Gator were filed. During 2002, Six Continents Hotels Inc. and Inter-Continental Hotels Corp. sued Gator in Atlanta for copyright and trademark infringement, unfair competition, and computer trespass, and Extended Stay America Inc. (ESA) sued Gator in South Carolina on similar grounds. Gator, in turn, sued ESA for declaratory relief in federal court in San Jose, California.⁴³⁶¹ In May 2003, LendingTree Inc. sued Gator for copyright and trademark infringement, asking for statutory damages of \$150,000 for each infringement.⁴³⁶² As of the writing of this paper, these suits were pending.

2. The WhenU Litigations

Several lawsuits have been brought against WhenU.com, distributor of a pop-up ad program called “SaveNow,” alleging copyright and trademark infringement. Although the cases reached similar results on the copyright claims, they reached different results on the trademark claims.

(a) U-Haul v. WhenU.com

In U-Haul Int’l Inc. v. WhenU.com, Inc.,⁴³⁶³ U-Haul alleged that WhenU’s SaveNow pop-up ad program constituted copyright and trademark infringement and unfair competition. SaveNow was generally bundled for distribution with other software programs, such as screensaver programs. It was distributed with a clickwrap license agreement. Utilizing a directory of commonly used search phrases, commonly visited web addresses, and various keyword algorithms, the SaveNow program scanned the user’s Internet activity to determine whether any of the terms, web addresses, or content matched the information in its directory. Upon detecting a match, the program identified an associated product or service category, and then caused a pop-up advertisement to be selected from WhenU’s clients which matched the category of the user’s activity. The ads appeared in a separate “WhenU window” on top of all

⁴³⁵⁹ Order granting preliminary injunction, Washingtonpost.Newsweek Interactive Co. v. The Gator Corporation, Civil Action 02-909-A (E.D. Va. July 16, 2002) (copy on file with the author). The court also enjoined Gator from infringing the plaintiffs’ trademark or service mark rights, and from making any designations of origin, descriptions, representations or suggestions that the plaintiffs were the source, sponsor or in any way affiliated with Gator’s advertisers or their web sites, services and products.

⁴³⁶⁰ “Settlement Reportedly Reached in Dispute Over Pop-Up Advertisements,” *Mealey’s Litigation Report: Intellectual Property* (Feb. 17, 2003), at 22.

⁴³⁶¹ Lisa Shuchman, “Search and Destroy” (Jan. 16, 2003), available as of Jan. 18, 2003 at www.law.com/jsp/article.jsp?id=1039054570236.

⁴³⁶² Jen Zoghby, “LendingTree Suit Pops Pop-Ups” (May 19, 2003), available as of Oct. 26, 2003 at <http://famulus.msnbc.com/famuluscom/bizjournal05-19-010109.asp>.

⁴³⁶³ 2003 WL 22071556 (E.D. Va. 2003).

other windows visible on the computer's screen, including the window of the user's selected destination web site.⁴³⁶⁴

The court rejected U-Haul's arguments that SaveNow infringed its exclusive rights of display and derivative works. With respect to the display right, U-Haul argued that SaveNow unlawfully caused its web site to be displayed together with WhenU's pop-up ads. The court rejected this argument, noting that the user, not SaveNow, was the one who called up the U-Haul website. The SaveNow program did not alter U-Haul's web page in any manner, and the SaveNow window in which the ad appeared bore no physical relationship to the window in which the U-Haul web page appeared.⁴³⁶⁵

With respect to the derivative works right, U-Haul argued that the SaveNow program created an infringing derivative work by retrieving the U-Haul web page, placing its own advertisement on that Web page, then displaying it to the user. The court ruled that no derivative work of the U-Haul web page was created. First, the WhenU window was a "distinct occurrence" from the U-Haul web page, rather than a single integrated work, and the appearance of a WhenU ad on the user's computer screen at the same time as a U-Haul web page was "a transitory occurrence that may not be exactly duplicated in that or another user's computer."⁴³⁶⁶ Second, although the pop-up ad altered the user's computer display, the alteration was not infringing. "To conclude otherwise is untenable in light of the fact that the user is the one who controls how items are displayed on the computer, and computer users would infringe copyrighted works any time they opened a window in front of a copyrighted Web page that is simultaneously open in a separate window on their computer screens."⁴³⁶⁷

Accordingly, WhenU was entitled to summary judgment on U-Haul's claim of copyright infringement.⁴³⁶⁸ The court also rejected U-Haul's trademark claim on the ground, among others, that the appearance of WhenU's ads on a user's computer screen at the same time as the U-Haul web page was a result of how applications operate in the Windows environment and therefore did not constitute a "use" of U-Haul's trademarks under the Lanham Act. Neither did inclusion of the U-Haul URL or the word "U-Haul" in the SaveNow program constitute "use" under the Lanham Act, particularly since WhenU did not sell the U-Haul URL to its customers or cause the U-Haul URL or name to be displayed to the computer user when the ads popped up.⁴³⁶⁹ Finally, the court found no unfair competition because the user had consented, by

⁴³⁶⁴ Id. at *2.

⁴³⁶⁵ Id. at *6.

⁴³⁶⁶ Id. at *7.

⁴³⁶⁷ Id.

⁴³⁶⁸ Id.

⁴³⁶⁹ Id. at 4.

accepting the clickwrap license and downloading the software, to the display of the ads on his or her screen.⁴³⁷⁰

(b) Wells Fargo v. WhenU.com

Similar claims of copyright and trademark infringement were brought against WhenU in the case of Wells Fargo & Co. v. WhenU.com, Inc.⁴³⁷¹ The court denied a motion for a preliminary injunction, finding that the plaintiffs had not shown a likelihood of success on the merits of either the copyright or the trademark claims. With respect to the copyright claims, the plaintiffs argued that the SaveNow program caused infringing derivative works of their websites to be created. The court ruled that, to support a claim of direct derivative works infringement against WhenU, the plaintiffs would need to prove that WhenU incorporated the plaintiffs' websites into a new work. The court ruled that the plaintiffs could not establish such proof, because WhenU merely supplied a software product that did not access the plaintiffs' websites and therefore did not incorporate them into a new work. Accordingly, the plaintiffs' claim for copyright infringement could, at best, be a claim for contributory infringement based on an allegedly infringing derivative work created by users of the WhenU software.⁴³⁷²

The court concluded that SaveNow users did not create infringing derivative works either. Use of the SaveNow program to display ads did not alter the plaintiffs' websites, nor did the WhenU ad window have any physical relationship to the plaintiffs' websites or alter the content displayed in any other open window.⁴³⁷³ Even if the presence of an overlapping window could be said to change the appearance of the underlying window on a computer screen, the court held that such alteration was not an infringement by analogy to the case of Lewis Galoob Toys v. Nintendo of Am.⁴³⁷⁴ That case held that the "Game Genie" device, which attached to the Nintendo game console and allowed players to temporarily alter certain attributes of video games, did not create a fixed derivative work because once the Game Genie was detached or the power turned off, the changes disappeared and the video game reverted to its original form.⁴³⁷⁵

By analogy, the court ruled that WhenU's program only temporarily changed the way the plaintiffs' websites were viewed by users, and as soon as the ad windows were closed or minimized, the plaintiffs' websites reverted to their original form.⁴³⁷⁶ The court also rejected the plaintiffs' argument that an unauthorized derivative work was formed because the WhenU ads modified the pixels on the user's screen display. The court concluded that the pixels "are owned and controlled by the computer user who chooses what to display on the screen" and the

⁴³⁷⁰ Id. at *1.

⁴³⁷¹ 293 F. Supp. 2d 734 (E.D. Mich. 2003).

⁴³⁷² Id. at 769.

⁴³⁷³ Id.

⁴³⁷⁴ 780 F. Supp. 1283 (N.D. Cal. 1991), aff'd, 964 F.2d 965 (9th Cir. 1992).

⁴³⁷⁵ Id. at 1288, 1291.

⁴³⁷⁶ Wells Fargo, 293 F. Supp. 2d at 770.

plaintiffs' did not have any property or copyright interest in those pixels.⁴³⁷⁷ The court also noted that because the pixels on a computer screen are updated every 1/70th of a second, the "alteration of pixels is therefore far too transitory an occurrence to form a basis for a copyright violation."⁴³⁷⁸ The court therefore ruled that the WhenU advertisements did not create a work sufficiently permanent to be independently copyrightable, and therefore did not create a derivative work.⁴³⁷⁹

With respect to the plaintiffs' trademark claims, the court rejected three arguments made by the plaintiffs as to why WhenU should be found to "use" the plaintiffs' trademarks in commerce, as required to establish a violation of the Lanham Act. First, the plaintiffs argued that WhenU hindered Internet users from accessing their websites by potentially diverting them to other sites when the user entered the URL of their websites, and such diversion constituted a "use" of their trademarks. The court rejected this argument, noting that WhenU used the plaintiffs' trademarks only in its software directory, to which the typical consumer did not have access, and entry of the plaintiffs' URLs in fact directed them to the plaintiffs' web sites.⁴³⁸⁰

Second, the plaintiffs argued that WhenU positioned its pop-up ads in such a way that consumers would see one display containing WhenU's ads and the plaintiffs' websites and trademarks. This positioning, the plaintiffs argued, created the impression that the pop-up was affiliated with or approved by the plaintiffs. The court rejected this argument, finding that it was apparent to the user that what was appearing on his or her screen was two distinct sources of material. The court noted that the plaintiffs' marks were neither displayed nor appeared to be displayed on WhenU's windows, and the fact that WhenU's ads appeared on a computer screen at the same time the plaintiffs' web pages were visible in a separate window was not a "use" in commerce of the plaintiffs' marks.⁴³⁸¹ Instead, the court concluded it was a form of legitimate comparative advertising.⁴³⁸²

Finally, the plaintiffs argued that the inclusion of their trademarks in WhenU's software directory was a use in commerce. The court rejected this argument as well, finding that the directory entries were used only to identify the category of material a user was interested in, and to dispatch a contextually relevant ad to that user. The ad did not display the plaintiffs'

⁴³⁷⁷ Id. at 770-71.

⁴³⁷⁸ Id. at 771.

⁴³⁷⁹ Id.

⁴³⁸⁰ Id. at 758-59.

⁴³⁸¹ Id. at 759-61.

⁴³⁸² Id. at 761.

trademarks, and WhenU did not use the plaintiffs' trademarks to indicate anything about the source of the products and services it advertised.⁴³⁸³

(c) 1-800 Contacts v. WhenU.com

A third opinion in the various litigations against WhenU was issued just one month after the Wells Fargo opinion. In the case of 1-800 Contacts, Inc. v. WhenU.com,⁴³⁸⁴ the district court reached the same conclusion as the U-Haul and Wells Fargo courts on the copyright claims, but reached an opposite conclusion on the trademark claims, although its trademark ruling was later reversed on appeal to the Second Circuit. In this case, claims were brought against both WhenU and one of its advertising customers, Direct Vision, a competitor of the plaintiff 1-800 Contacts. In addition to the copyright and trademark claims, the plaintiff asserted a violation of the Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d).

With respect to its claim of copyright infringement, the plaintiff argued that, by delivering pop-up ads to a SaveNow user's computer while the user was viewing the plaintiff's website, the defendants created a new screen display that incorporated the plaintiff's copyrighted work, thereby infringing the plaintiff's exclusive right of display.⁴³⁸⁵ The court rejected this argument, finding that it would prove way too much were it accepted:

For this court to hold that computer users are limited in their use of Plaintiff's website to viewing the website without any obstructing windows or programs would be to subject countless computer users and software developers to liability for copyright infringement and contributory copyright infringement, since the modern computer environment in which Plaintiff's website exists allows users to obscure, cover, and change the appearance of browser windows containing Plaintiff's website. Without authority or evidence for the claim that users exceed their license to view the copyrighted 1-800 Contacts website when they obscure the website with other browser windows (including pop-up ads generated by the SaveNow program), Plaintiff has little basis for its claim that Defendants have infringed its display right.⁴³⁸⁶

The court also rejected the plaintiff's argument that the defendants were creating unauthorized derivative works by adding to or deleting from its copyrighted website, thereby

⁴³⁸³ Id. at 762. The court also ruled that the plaintiffs had not demonstrated a likelihood of success on the issue of confusion. The court found a number of flaws in the survey conducted by the plaintiffs' expert, in that it did not approximate actual market conditions, did not survey the appropriate population, contained questions that were unclear and leading, and contained no control questions. Id. at 765-69. In March of 2003, plaintiffs Wells Fargo and Quicken Loans settled their lawsuit against WhenU.com and filed a stipulated order of dismissal. See "Wells Fargo Settles WhenU.com Pop-Up Ads Case," *BNA's Electronic Commerce & Law Report* (Mar. 30, 2005) at 329.

⁴³⁸⁴ 309 F.Supp.2d 467 (S.D.N.Y. 2003).

⁴³⁸⁵ Id. at 485.

⁴³⁸⁶ Id.

“transforming” or “recasting” the website.⁴³⁸⁷ Similar to the holdings in the U-Haul and Wells Fargo cases, the court found that no derivative work satisfying the fixation requirement was created by the SaveNow program, in view of the fact that the pop-up ads could be moved, obscured, or closed entirely, thus disappearing from perception, with the single click of a mouse.⁴³⁸⁸ In addition, to the extent the pop-up ads constituted “transmitted images,” they were not fixed works since there was no evidence that a fixation was made “simultaneously with” the pop-up ads’ “transmission,” as required by the definitions in section 101 of the copyright statute.⁴³⁸⁹ Finally, the court ruled that the defendants had not recast or transformed the plaintiff’s website because its website remained intact on the computer screen. Although the defendants’ pop-up ads might obscure or cover a portion of the website, they did not change it.⁴³⁹⁰

Moreover, if obscuring a browser window containing a copyrighted website with another computer window produced a “derivative work,” then any action by a computer user that produced a computer window or visual graphic that altered the screen appearance of Plaintiff’s website, however slight, would require Plaintiff’s permission. A definition of “derivative work” that sweeps within the scope of the copyright law a multi-tasking Internet shopper whose word-processing program obscures the screen display of Plaintiff’s website is indeed “jarring,” and not supported by the definition set forth at 17 U.S.C. § 101.⁴³⁹¹

The district court, however, reached an opposite conclusion to the U-Haul and Wells Fargo courts on the issue of trademark infringement, expressly noting that it disagreed with those courts.⁴³⁹² Unlike those courts, the 1-800 Contacts court found that the defendants were making “use” of the plaintiff’s trademarks in commerce for several reasons. First, SaveNow users that typed in the plaintiff’s web site address or its 1-800 CONTACTS trademark in a search were exhibiting a prior knowledge of the plaintiff’s website or goods and services, and the court found that pop-up ads that capitalized on that knowledge were “using” the plaintiff’s marks that appeared on its website.⁴³⁹³ Second, the court found that by including the plaintiff’s URL, www.1800contacts.com, in its software directory of terms that triggered pop-up ads, WhenU was “using” a version of the plaintiff’s 1-800 CONTACTS mark.⁴³⁹⁴ Thus, the court concluded that, by delivering ads to a SaveNow user when the user directly accessed the plaintiff’s website, the SaveNow program allowed the defendant Vision Direct, to profit from the goodwill and

⁴³⁸⁷ Id. at 486.

⁴³⁸⁸ Id. at 487.

⁴³⁸⁹ Id.

⁴³⁹⁰ Id.

⁴³⁹¹ Id. at 487-88.

⁴³⁹² Id. at 490 n.43.

⁴³⁹³ Id. at 489.

⁴³⁹⁴ Id.

reputation in the plaintiff's website that led the user to access the plaintiff's website in the first place.⁴³⁹⁵

With respect to the issue of confusion, although the court found the survey of the plaintiff's expert, which was the same expert as the Wells Fargo case, to be flawed for many of the same reasons the Wells Fargo court noted, the court nevertheless held that the plaintiff had established a sufficient showing of likelihood of harm from both "initial interest confusion" and "source confusion" to support a Lanham Act claim.⁴³⁹⁶ The court also ruled that, by registering the domain name www.www1800Contacts.com, the defendant Vision Direct had violated the Anticybersquatting Consumer Protection Act.⁴³⁹⁷

Accordingly, based on the trademark and anticybersquatting claims, the court entered a preliminary injunction against the defendants, enjoining them from (1) including the 1-800 CONTACTS mark, and confusingly similar terms, as elements in the SaveNow software directory, and (2) displaying the plaintiff's mark in the advertising of Vision Direct's services, by causing "Vision Direct's pop-up advertisements to appear when a computer user has made a specific choice to access or find Plaintiff's website by typing Plaintiff's mark into the URL bar of a web browser or into an Internet search engine."⁴³⁹⁸

On interlocutory appeal of the preliminary injunction, the Second Circuit reversed, ruling that as a matter of law WhenU did not "use" the plaintiff's marks within the meaning of the Lanham Act when it included the plaintiff's URL in its software directory or when it caused separate, branded pop-up ads to appear either above, below, or along the bottom edge of the plaintiff's website window.⁴³⁹⁹ With respect to inclusion of the URL in WhenU's directory, the Second Circuit ruled that the URL transformed the plaintiff's trademark into a word combination that functioned more or less like a public key to the plaintiff's website. The only place WhenU reproduced the address was in its directory, which was not accessible to users and could therefore not create a possibility of visual confusion with the plaintiff's mark. In addition, a WhenU pop-up ad could not be triggered by a computer user's input of the 1-800 trademark or the appearance of that trademark on a web page accessed by the user. Accordingly, the court ruled that WhenU's inclusion of the 1-800 web address in its directory did not infringe on the plaintiff's trademark.⁴⁴⁰⁰

With respect to the pop-up ads, the court noted that they appeared in a separate window prominently branded with the WhenU mark and had no tangible effect on the appearance or functionality of the plaintiff's website. Nor was the appearance of the ads

⁴³⁹⁵ Id. at 490.

⁴³⁹⁶ Id. at 490-505.

⁴³⁹⁷ Id. at 505-07.

⁴³⁹⁸ Id. at 510.

⁴³⁹⁹ 1-800 Contacts, Inc. v. Whenu.com, Inc., 414 F.3d 400, 403 (2d Cir.), cert. denied, 126 S. Ct. 749 (2005).

⁴⁴⁰⁰ Id. at 408-09.

contingent upon or related to the plaintiff's trademark, the trademark's appearance on the plaintiff's website, or the mark's similarity to the plaintiff's web address. Rather, the display of the ads was the result of the happenstance that the plaintiff chose to use a mark similar to its trademark as the address to its web page. Nor did WhenU's activities divert or misdirect computer users away from the plaintiff's website. Finally, the court noted that WhenU did not sell keyword trademarks to its customers or otherwise manipulate which category-related ad would pop up in response to any particular terms on the internal directory. Accordingly, the ads did not represent a "use" in commerce of the plaintiff's trademarks.⁴⁴⁰¹

3. The MetroGuide Litigation

In January 2003, MetroGuide.com sued Hotels.com in Florida for violations of copyright and unfair competition laws for its practice of causing pop-up ads for Hotels.com to appear over MetroGuide's web sites. The complaint alleges that the pop-up ads obscured the plaintiff's brand and content underneath them, enticing customers to book rooms directly with Hotels.com.⁴⁴⁰²

4. The D Squared Litigation

In Oct. 2003, the Federal Trade Commission instituted litigation against D Squared Solutions in federal district court in Maryland.⁴⁴⁰³ D Squared co-opted a network administration feature of Microsoft Windows known as "Messenger Service," which was designed to enable computer network administrators to provide instant information to network users such as the need to log off, to send a stream of repeated pop-up advertisements that appeared on the screens of computer users connected to the Internet at 10- to 30-minute intervals. The pop-up messages instructed consumers to visit one of the defendants' web sites to purchase software that would cause the pop-up ads to stop.⁴⁴⁰⁴ The FTC sued D Squared, alleging that its business methods constituted unfair competition, and secured a temporary restraining order against the defendants.⁴⁴⁰⁵

On Dec. 16, 2003, the court, after a hearing on an order to show cause why the court should not enter a preliminary injunction, denied the FTC's request for a preliminary injunction, vacated the temporary restraining order, and directed counsel to commence discovery immediately. A non-jury trial was calendared for Mar. 8-10, 2004. Because the court rendered its ruling on the record, no opinion was issued giving the court's reasons. However, the court

⁴⁴⁰¹ *Id.* at 410-12.

⁴⁴⁰² "MetroGuide.com Sues Hotels.com; Seeks Damages for Copyright Infringement and Predatory Advertising" (Jan. 27, 2003), available as of Jan. 28, 2003 at www.businesswire.com/cgi-bin/f_headline.cgi?bw.012703/230272653.

⁴⁴⁰³ Complaint, *Federal Trade Commission v. D Squared Solutions, LLC*, 03 CV 31 08 (D. Md. Oct. 30, 2003), available as of Jan. 17, 2004 at www.ftc.gov/os/2003/11/0323223comp.pdf.

⁴⁴⁰⁴ *Id.* ¶¶ 9-10.

⁴⁴⁰⁵ The temporary restraining order was available as of Jan. 17, 2004 at www.ftc.gov/os/2003/11/0323223tro.pdf.

apparently noted that it was unclear whether the pop-up ads had caused substantial injury to consumers.⁴⁴⁰⁶ As of the writing of this paper, the litigation was ongoing.

5. International Decisions

In March of 2004, a the Court of First Instance in Cologne, Germany, issued a preliminary injunction against Claria (formerly known as Gator) that prohibited the company's pop-up and pop-under ads from appearing over Hertz's German rental car web site. The court concluded that Claria had violated various sections of a German unfair competition law.⁴⁴⁰⁷

H. Harvesting of Web Data

Harvesting of web data using robots and subsequent use or posting of the harvested data is a common occurrence on the Web and can be expected to generate much litigation in the future over claims of copyright infringement and the DMCA. A number of cases are beginning to emerge:

1. The FatWallet Dispute

Shortly before Thanksgiving of 2002, FatWallet.com posted on its web site a list of products and prices scheduled to appear in advertisements on "Black Friday" (the day after Thanksgiving, when by urban legend retailers go "in the black" and start to make money). The products and prices had apparently been harvested from web sites of various retailers. Wal-Mart, one of the companies whose data had been harvested, wrote a letter to FatWallet demanding the takedown under the DMCA of its product and pricing data on the ground that such data constituted a copyrighted compilation. Wal-Mart's attorneys also issued a subpoena under Section 512(h) of the DMCA asking for "information sufficient to identify the individual who posted the infringing material." Wal-Mart backed down on its demands after the Samuelson Law, Technology & Public Policy Clinic at Boalt Hall School of Law agreed to represent FatWallet and fight the subpoena.⁴⁴⁰⁸

2. Nautical Solutions Marketing v. Boats.com

Boats.com operated a web site, Yachtworld.com, on which subscribing yacht brokers posted listings of yachts for sale. Nautical Solutions Marketing (NSM) opened a competing web site known as Yachtbroker.com. NSM offered two services that Boats.com alleged were infringing of its copyrights. First, NSM used an Internet spider called Boat Rover to extract public yacht listing data from Yachtworld.com and other sites, such as manufacturer, model, length,

⁴⁴⁰⁶ "FTC Denied Injunction Against Software Firm's Intrusive Pop-Up Ads" (Dec. 15, 2003), available as of Jan. 17, 2004 at <http://24hour.startribune.com/24hour/technology/story/1089101p-7607955c.html>.

⁴⁴⁰⁷ Dawn Kawamoto, "German Court: Pop-Ups Need Permission" (Mar. 26, 2004), available as of Mar. 29, 2004 at www.news.com.com/2100-1024_3-5180240.html.

⁴⁴⁰⁸ Declan McCullagh, "Wal-Mart Backs Away from DMCA Claim" (Dec. 5, 2002), available as of Dec. 8, 2002 at <http://news.com.com/2102-1023-976296.html>.

year of manufacture, price, location, and URL of the web page containing the yacht listing. Boat Rover extracted the facts by momentarily copying the HTML of the web page containing the yacht listing and then collecting the prescribed facts, entering the facts into a searchable database, and then discarding the HTML.⁴⁴⁰⁹

Second, NSM offered a “valet service” under which, with the permission of a yacht broker who owned a yacht listing on another web site, it would move, delete or modify the yacht broker’s listing. Under this service, Yachtbroker.com copied and pasted certain content, including pictures and descriptions (but not the HTML for the entire web page), from yacht listings on Yachtworld.com and posted the content on Yachtbroker.com in a different format. Although the copied content posted on Yachtbroker.com contained many of the same descriptive headings as the original listings on Yachtworld.com, the court found that the headings were the industry standard for yacht listings on yacht brokering web sites.⁴⁴¹⁰

NSM filed an action for a declaratory judgment that its two services did not infringe Boats.com’s copyrights, which the court granted. The court ruled that Boats.com’s copyright of Yachtworld.com’s public web pages in order to extract from yacht listings facts unprotected by copyright law constituted a fair use.⁴⁴¹¹ The court further ruled that the copyrights in the pictures and descriptions of yachts copied by the valet service were owned by the individual yacht brokers, not Boats.com, and such copying was therefore not infringing. Nor was copying of the headings an infringement, because the headings, being industry standards, were not protected by copyright.⁴⁴¹² Boats.com also claimed a copyright in the look and feel of the Yachtworld.com web site that it alleged had been copied by Yachtbroker.com. The court rejected this claim, finding that the two web sites were quite dissimilar in appearance.⁴⁴¹³ Finally, the court rejected a claim of infringement in a compilation copyright over the yacht listings on Yachtworld.com. The court held that, because the format used by NSM to display on Yachtbroker.com the content copied from Yachtworld.com differed from the format used by Yachtworld.com to display the same information, the compilation of yacht listings on Yachtbroker.com was not virtually identical and was therefore not infringing.⁴⁴¹⁴

3. Craigslist v. 3Taps

In this case, Craigslist brought claims, among others, of copyright infringement against a number of defendants based on their activity of aggregating and republishing ads from Craigslist and, in the case of the defendant 3Taps, marketing a “Craigslist API” that allowed third parties to

⁴⁴⁰⁹ Nautical Solutions Marketing, Inc. v. Boats.com, No. 8:02-cv-760-T-23TGW (M.D. Fla. Apr. 2, 2004), slip op. at 1-2.

⁴⁴¹⁰ Id. at 3-4.

⁴⁴¹¹ Id. at 4.

⁴⁴¹² Id. at 5.

⁴⁴¹³ Id. at 6.

⁴⁴¹⁴ Id. at 7.

access large amounts of content from Craigslist. The defendants brought a motion to dismiss on the ground that neither the individual ad postings nor Craigslist's compilation of them were copyrightable. The court rejected the motion, ruling that Craigslist had adequately alleged that its users' ads had a level of creativity that was not trivial and therefore sufficiently original to fall within the scope of copyright protection. It also ruled that the allegations in the complaint that Craigslist had decided which categories of ads to include on its web site and under what name were sufficient to demonstrate a minimal level of creativity to establish that Craigslist could potentially have a copyright in the compilation of ads on its web site.⁴⁴¹⁵

The court concluded, however, that Craigslist had acquired sufficient license rights to have standing to enforce the copyrights in individual user-created ads only with respect to ads posted in the period from July 16, 2012 through August 8, 2012. During that period, users submitting ads were presented with a special notice stating that clicking "Continue" confirmed that Craigslist was the exclusive licensee of the content submitted, with the exclusive right to enforce against anyone copying, republishing, distributing or preparing derivative works without its consent. Outside that limited time period, Craigslist required a posting user to agree only to its general web site Terms of Use, which stated that the user granted a perpetual, irrevocable, unlimited license to copy, perform, display, distribute, prepare derivative works from and otherwise use any content posted by the user. Because the Terms of Use license was not stated as being exclusive, it was insufficient to give Craigslist standing to enforce the individual user ads.⁴⁴¹⁶

IV. CONCLUSION

Copyright law provides one of the most important forms of intellectual property protection on the Internet. Considerable challenges are presented, however, in adapting traditional copyright law, which was designed to deal with the creation, distribution and sale of protected works in tangible copies, to the electronic transmissions of the online world in which copies are not tangible in the traditional sense, and it is often difficult to know precisely where a copy resides at any given time within the network.

The most difficult aspect of adapting copyright law to the online world stems from the fact that virtually every activity on the Internet – such as browsing, caching, linking, downloading, accessing information, and operation of an online service – involves the making of copies, at least to the extent the law treats electronic images of data stored in RAM as "copies" for purposes of copyright law. In short, "copying" is both ubiquitous and inherent in the very nature of the medium. If the law were to treat all forms of "copying" as infringements of the copyright holder's rights, then the copyright holder would have very strong control over Internet use of the copyrighted work. Which forms of copying the law should deem to be within the control of the copyright owner and which should not presents a very difficult challenge.

⁴⁴¹⁵ Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 971-72 (N.D. Cal. 2013).

⁴⁴¹⁶ Id. at 972-74.

The cumulative effect of the copyright holder's rights being implicated by every use of a work on the Internet may be to give the copyright owner the equivalent of exclusive rights of "transmission and access" of information. Indeed, the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty each make such rights express. However, the DMCA does not set up separate rights of transmission and access, although the draft European Copyright Directive would recognize such rights explicitly. Thus, the implementing legislative regimes adopted by various signatory countries to the WIPO treaties may result in varying scopes and/or denominations of rights, which runs contrary to the goal of the WIPO treaties to harmonize copyright law in the digital environment throughout the world.

The ubiquitous nature of "copying" on the Internet raises other difficult issues. For example, the practice of dividing copyright rights (such as the reproduction right, the public performance right, and the distribution right) among separate rights holders, as is common in the movie and music industries, will raise difficult issues of overlapping rights when a work is exploited through the Internet, because the exercise of all such rights will involve the making of "copies." Licensees may therefore need to seek permission from multiple rights holders that may not have been necessary in traditional media.⁴⁴¹⁷

Moreover, the traditional divisions of the bundle of copyright rights may no longer make sense on the Internet. For example, it is common for different entities to hold the right to reproduce copies of a movie, to distribute copies of the movie, and to grant licenses for public performance of the movie. Under that division of rights, who has the right to make the movie available on the Internet for on-demand viewing by users, since on-demand viewings will involve the making of copies of the movie, the distribution of copies, and the public performance of the movie? Or should it be the holder of the new right of transmission and access under the WIPO treaties?⁴⁴¹⁸ Because of the overlapping nature of copyright rights when applied to the Internet, new definitions and divisions of those rights will probably be necessary for online usage of copyrighted works. Corresponding new economic and royalty models and industry practices will also have to evolve. In the meantime, many existing licenses will be unclear as to which entity has rights to control online usage of a work, and one can expect to see much litigation over the interpretation of existing licenses.⁴⁴¹⁹

⁴⁴¹⁷ See Lemley, *supra* note 6, at 568-72.

⁴⁴¹⁸ Because the new right of transmission and access in the WIPO treaties will be in addition to the other rights that may be implicated by Internet uses of copyrighted works, these new rights can be expected to increase the problem of overlapping rights. For example, existing licenses will be silent on these new rights, and there will therefore be great uncertainty as to whether the licensor retains such rights, or whether the licensee has a license under such rights and, if so, of what scope.

⁴⁴¹⁹ See Lemley, *supra* note 6, at 572-74. One commentator has considered several possible ways of dealing with the overlap of exclusive copyright rights that occurs on the Internet (placing the burden of overlap on the user; placing the burden of overlap on the copyright owner; and establishing a new right of transmission over a computer network that would *replace* the other rights to the extent they are applicable to network transmissions). See *id.* at 578-84.

The global nature of the Internet may give rise to multiple territorial liability. If every intermediate “copy” made during a transmission is considered infringing, there is the possibility that a single transmission could give rise to potential liability in several countries, even countries in which the sender did not intend or contemplate that its actions would result in the creation of a copy.⁴⁴²⁰ Moreover, differing standards could apply – the same intermediate copy created in the course of transmission through the Internet could be considered infringing when passing through one country, and not when passing through another. In addition, the violation of the rights of transmission and access under the WIPO treaties might occur in yet another country. Although the WIPO treaties may afford a vehicle for greater transnational uniformity of copyright law, there is no guarantee that implementing legislation in the various signatory countries will be consistently adopted, consistently interpreted, or consistently applied.

In sum, copyright owners may have potentially unprecedented rights over use of their copyrighted material on the Internet. One can expect that the fair use and implied license doctrines (and their international equivalents) will take center stage in resolving the balance between copyright owners’ and users’ rights on the Internet. How broadly these doctrines will be applied, and whether they will be consistently applied in various countries, will be a process of constant evolution. Copyright lawyers will continue to be busy.

⁴⁴²⁰ In addition, at least one court held that where predicate acts occurred in the U.S. leading to infringements that occurred abroad, damages flowing worldwide from a U.S. infringement could be considered. Update Art, Inc. v. Modiin Publishing, Ltd., 843 F.2d 67 (2d Cir. 1988).