FENWICK & WEST LLP

Notable New Cases in Copyright/ DMCA Litigation (2005-2006)

Originally published in the *Practicing Law Institute* course book, Understanding Basic Copyright Law, 2006.

MITCHELL ZIMMERMAN

FENWICK & WEST LLP

About the Firm

Fenwick & West LLP provides comprehensive legal services to high technology and biotechnology clients of national and international prominence. We have over 250 attorneys and a network of correspondent firms in major cities throughout the world. We have offices in Mountain View and San Francisco, California.

Fenwick & West LLP is committed to providing excellent, cost-effective and practical legal services and solutions that focus on global high technology industries and issues. We believe that technology will continue to drive our national and global economies, and look forward to partnering with our clients to create the products and services that will help build great companies. We differentiate ourselves by having greater depth in our understanding of our clients' technologies, industry environment and business needs than is typically expected of lawyers.

Fenwick & West is a full service law firm with nationally ranked practice groups covering:

- Corporate (emerging growth, financings, securities, mergers & acquisitions)
- Intellectual Property (patent, copyright, licensing, trademark)
- Litigation (commercial, IP litigation and alternative dispute-resolution)
- Tax (domestic, international tax planning and litigation)

Intellectual Property Group

Fenwick & West's Intellectual Property Group offers comprehensive, integrated advice regarding all aspects of the protection and exploitation of intellectual property. From providing sophisticated legal defense in precedent-setting user interface copyright lawsuits to prosecuting arcane software patents, and from crafting user distribution arrangements on behalf of high technology companies to implementing penetrating intellectual property audits, our attorney's technical skills enable the Firm to render sophisticated legal advice.

Our Offices

Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel: 650.988.8500
Fax: 650.938.5200

Embarcadero Center West
275 Battery Street
San Francisco, CA 94111
Tel: 415.875.2300
Fax: 415.281.1350

Wells Fargo Center
877 West Main Street, Suite 706
Boise, ID 83702
Tel: 208.331.0700
Fax: 208.331.7723

For more information about Fenwick & West LLP, please visit our Web site at: www.fenwick.com.

Notable New Cases in Copyright/DMCA Litigation (2005-2006)

Table of Contents

Introduction

The year 2005-06 has seen a substantial group of decisions – including some cases of first impression – that flesh out the law of primary and secondary liability, fair use and various other copyright defenses, as well as further defining the application of the anti-circumvention and copyright management information provisions of the Digital Millennium Copyright Act.

Internet Image Searching & Fair Use

Perfect 10 v. Google, Inc., 416 F. Supp. 2d 828 (C.D. Cal. 2006) [1]

On February 21, 2006, a federal district court in Los Angeles issued two important rulings in a dispute between "adult" content provider Perfect 10 and the leading internet search company, Google, Inc. In an important case of first impression, the court held first that Google's web page "framing" does not constitute copyright infringement. Next, in a ruling seemingly at odds with a less-than-three-years-old holding of the Ninth Circuit, the district court held that Google's display of "thumbnail" versions of Perfect 10 photographs in image search results was not a fair use.

Case Background. Plaintiff Perfect 10 ("P10") distributes original erotic photographs of "natural" models via its adult web site and magazine and as downloads for cell phone wallpaper. Many of these copyrighted images have been copied and displayed, without P10's permission, on other web sites. Those web sites, and their infringing photographs, are automatically cataloged by Google's search engine function.

In 2004, Google launched an image searching function. In response to searches for various terms, Google displays results as a grid array of "thumbnail"-sized images responsive to the search. Clicking on a thumbnail opens a new window with a Google heading at the top and a section on the bottom of that shows a full-size image of the underlying web page where the searched-for image was found, framed within a Google-generated web page. The "Google" section of the web page also offers a link that can cause the user to leave the Google site altogether and go to the site where the original was found.

The process of creating such pages is called framing or in-line linking. The image, though shown within the Google frame on the user's computer, is actually delivered as the result of an automated link within Google's web page. In other words, the internet user's browser reads a computer software code that Google delivers along with its part of the page and then, pursuant to the instructions contained in that code, calls up the underlying web page where the image originated, and inserts that underlying page into the Google-supplied frame. The actual full-sized image, consequently, is not stored on Google's server, but on that of the original source web site.

In the example below, an image search for “Bill Fenwick” generated a web page with the following results.

When the user clicked on the second image, a new web page appeared (see below) that displayed both Google’s section (including a thumbnail-sized image of a painting by artist Bill Fenwick) and a section showing the web page from which the image of the painting was found.

Plaintiff Perfect 10 objected when various image searches generated results that included copies of its photographs that were hosted on infringing web sites. After sending a series of infringement notices to Google, P10 filed suit in November 2004, alleging *inter alia* that Google's display of thumbnail images and its framing of the underlying infringing web sites constituted direct, contributory and vicarious copyright infringement.

Perfect 10 moved for a preliminary injunction on the copyright claims. In its February 2006 Order, a Federal District Court in the Central District of California granted relief in part to Perfect 10. The key holdings in the case were:

- The presentation of images through frames did not violate Perfect 10's display right;
- The display of thumbnail copies of P10 photographs for search purposes did not represent fair use;
- Google is not liable for contributory infringement because the search capacity does not "materially contribute" to infringements;
- Google is not vicariously liable because it exercised no control over infringing activity.

Direct infringement: Framing. From the perspective of the end-user, P10 argued, when an image search is performed and the results displayed, it looks as though Google is displaying the pages containing the infringing photo, and (P10 alleged) the resulting framed images violated its exclusive display right concerning those photographs. Google responded that the framed image were not Google's display, because in reality all that Google was presenting was a link that would allow the end user's browser to integrate part of a web page from Google with a portion of the original web page which is downloaded from the original web site, and not from Google's server.

The Court observed that there were two alternative tests that could be employed to decide who was engaging in the display of the work that appears in a frame.

Under *the server test*, the owner of the computer server that actually hosts the image being transmitted to end users would be deemed the party that was engaging in the display.

Alternatively, under the *incorporation test*, the owner of the server that caused the end user's computer to incorporate the image into a web page on the end user's screen would be deemed the one engaging in the display.

The Court noted the potentially chilling effect of the incorporation test on all internet linking, and held the server test to be more appropriate. The Court employed the server test – under which Google was not liable for the displays – for a number of reasons: because the server

test better reflected technical realty; because it neither invited infringing activity nor wholly immunized Google from potential liability for infringing activity (Google might in theory still face secondary liability); because it was less ambiguous and more easily applied by web site operators; because even under that test, other direct infringers can be identified against whom relief could be sought; and because the server test maintained "the delicate balance for which copyright law strives – *i.e.* between encouraging the creation of creative works and encouraging the dissemination of information."

The bottom line: Google had not engaged in a display of Perfect 10's work.

Thumbnails. Less that three years ago, the Ninth Circuit addressed the issue of thumbnail copying for image search engine purposes in *Kelly vs. Arriba Soft*, 336 F.3d 811 (9th Cir. 2003). In *Kelly*, the Court of Appeals engaged in the traditional four-part fair use analysis, and concluded that copying for such purposes was fair use. The key considerations: making copies for search purposes was highly transformative, and there was no appreciable impact on the value of or market for the original works. That a district court could come to a contrary conclusion to its controlling higher court so soon after the *Kelly* decision is startling, to say the least. Depending on ones perspective, the District Court's decision in *Perfect 10* either represented thinly-veiled defiance of controlling authority or a sage recognition that subsequent changes in the market place and in the operation of the internet compelled a different outcome. The district court reasoned as follows:

Factor one: Purpose and Character of the Use. The court considered separately the commercial character of the use and whether its character was transformative. The Court held that the commercial character of Google's activities weighed somewhat against fair use, although not too heavily, because Google derives some commercial benefit from infringing uses of P10's images. Indeed, in some instances Google derived advertising revenue directly from the displays and click-throughs that occurred as a result of such displays because of its "AdSense" marketing program.

Next, the court considered whether the use was a transformative one, as opposed to a "consumptive" use, that is, a use that merely supersedes the objective of the original use. The inferior quality and small size of the thumbnail photos, the court found, did not supersede Perfect 10's market for full-sized images of P10 photographs, and Google's information location tools and function was highly transformative of the original entertainment purpose of those images with regard to full-sized imaged. However, Google's use of reduced-sized images of Perfect 10's photos was deemed consumptive.

In early 2005, after filing suit, Perfect 10 entered into a licensing agreement with Fonestarz Media Limited for the sale and distribution of reduced-sized P10 images for use in cell phones displays. End users' downloads of Google thumbnails would supersede the copyright holder's use of those thumbnails for cell phones, the court concluded, hence this factor weighed in

favor of Perfect 10, although only slightly so in light of the transformative nature of Google's activity.

Factor Two: the Nature of the Copyrighted Work also weighed slightly in favor of Perfect 10. On the one hand, the photos were generally creative; but the fact that they had previously been published tended to favor fair use.

Factor Three: the Amount and Substantiality of the Portion Used was held to favor neither party. While the entirety of the photos was taken, as in *Kelly*, this was no more than was necessary for the transformative search engine purpose.

Fourth: the Effect of Google's Use on the Market for or Value of the Works was harmful. The use harmed and was a substitute for Perfect 10's market for reduced size images for use in cell phones.

The court concluded that, not withstanding the "enormous public benefit that search engines such as Google provide," it was compelled by "reasoned analysis of the four fair use factors" to hold Google's thumbnails did not constitute fair use.

The nature of compulsion is not easy to grasp, since the court's approach seemed to reflect an unnecessarily mechanical weighing of factors, particularly since a single consideration – the claimed substitution effect – fed into both the first and fourth factors.
The court went on to consider and reject P10's claims that Google was secondarily liable.

Secondary Liability: Contributory Infringement. A finding of secondary copyright liability requires that (i) there be an *underlying direct infringement*, and that, (ii) *with knowledge* of that infringement, the defendant (iii) *materially assist* in the infringement. In assessing Google's alleged contributory liability, the Court separated two potential sets of direct infringers: end users who use search results; and third party web sites that had displayed infringing copies of P10 photos on their sites.

Based on an analysis that focused on the creation of allegedly infringing copies in the computer cache of the end user's computers (as opposed to their screen displays), the court concluded that the end users were not infringers because they had a fair use defense. Such uses of cached copies were non-commercial and transformative; no more was taken than was necessary "to achieve the objectives of decreasing network latency and minimizing unnecessary bandwidth usage"; and such cache copying would likely have a minimal impact on the potential market for the original work.

Not so, however, with respect to the third party sites, which were likely to be found to be direct infringers. Nonetheless, the court considered it unlikely P10 would prove Google contributorily liable. The court discussed, but never resolved, whether Google had sufficient knowledge for

contributory liability. Instead, the court decided that P10 was not likely to prove that Google materially contributed to the infringing activity.

Secondary Liability: Vicarious Infringement. A finding of vicarious copyright infringement requires, again, (i) an *underlying direct infringement*, and further (ii) that the defendant *directly benefit financially* from the infringing activity, and (iii) have *the right and ability to supervise and control* the infringing activity. Although Google did have a direct financial benefit from the infringing activity, as a result of its AdSense program, it had lacked control over infringing activity.

The removal of a link to an infringing site, the Court held, which was all that removing Google search results could achieve, does not render the infringing site inaccessible. The "right and ability to control" infringing activity "means having substantial input into or authority over the decision to serve or continue to serve infringing content." "There must be some form of control over or authority to stop or limit the infringing conduct itself." Since Google had no such control, it was not vicariously liable.

The Injunction. Based on the foregoing analysis, the Court held that Perfect 10 was likely to prevail on its direct infringement claim regarding the thumbnails photos. The Court was prepared to enter a preliminary injunction on the thumbnail images, and ordered the parties to propose language jointly that would appropriately balance the competing interests.

Impact of the Decision. Although the case is only at the preliminary injunction stage, this order has substantial implications. The ruling is highly positive for the innumerable web sites that provide linking and framing. It is the first case to actually decide whether framing constitutes direct infringement and the "server test" is a favorable one for those who import content from other web sites.

But the court's departure from the rule of *Arriba Soft* again demonstrates the vicissitudes of the fair use analysis – and shows a disturbing inability to rely even on relatively recent in-circuit court of appeal authority.

Caching as Fair Use

Field v. Google, Inc., 412 F.Supp.2d 1106 (D.Nev. 2006)

Plaintiff Field, the district court found, "decided to manufacture a claim for copyright infringement against Google in the hope of making money from Google's standard practice" of caching pages. (A "cache," in computer terms, refers to a temporary storage area where frequently accessed data can be stored for rapid access.) Over a three-day period, Field created 51 "works" (quasi-poetical doggerel), which he placed on his web site at

www.blakeswritings.com. Field took steps calculated to have his web pages indexed by Google's search robot program. Field also deliberately omitted to use a simple, industry-standard meta-tag that would have caused Google's programs *not* to create an archival copy of his web site. As a result, pursuant to Google's standard, automated processes, Google's software robots copied and stored Field's web pages in its cache for later automatic reproduction and distribution upon request of Google users.

Field alleged that Google, by allowing internet users to access these cached copies, violated his exclusive rights to reproduce and distribute copies of his works, and demanded $2.5 million in statutory damages.

Not surprisingly, on these unappealing facts the district court took a dim view of Field's claims. Interestingly, the court felt comfortable disposing of the case on summary judgment, dismissing Field's claims on multiple grounds.

No Direct Infringement Because No Volitional Acts by Google. Following the principles set forth in *Religious Tech. Ctr v. Netcom On-Line Commc'n Services, Inc.*, 907 F.Supp.2d 1361 (N.D. Cal. 1995), and more recently confirmed in *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544 (4th Cir. 2004), the district court held that direct infringement requires "volitional conduct on the part of the defendant." When a user requests a web page contained in the Google cache, however, "Google is passive in this process. Google's computers respond automatically to the user's request. . . . The automated, non-volitional conduct by Google in response to a user's request does not constitute direct infringement under the Copyright Act." 907 F.Supp.2d at 1115.

The court further held Google was entitled to summary judgment based on various defenses.

Implied License. Ordinarily, a copyright holder has no affirmative obligation to take steps that make infringement more difficult. In the unusual circumstances of this case, however, the court held that a license was implied from Field's failure to take steps that could easily have prevented the alleged infringement, when he knew copying would otherwise occur.

"Consent to use the copyrighted work need not be manifested verbally and may be inferred based on silence where the copyright holder knows of the use and encourages it." *Id*. at 1116. The "no archive" meta-gag is a highly publicized and well-known industry standard, and Field knew of it and knew Google would interpret his failure to use the meta-tag as permission to cache. "[W]ith knowledge of how Google would use the copyrighted works . . . and with knowledge that he could prevent [caching], Field instead made a conscious decision to permit it." Such conduct "is reasonably interpreted as the grant of a license."

Estoppel. The court held that Field intended Google to rely upon his silence by caching his web pages, that his silence induced Google to rely upon it, and that Google (ignorant of the true facts) detrimentally relied on Field's conduct by caching Field's site.

Fair Use. The court applied the traditional, statutory four fair use factors (plus one), and found Google was entitled to summary judgment that its use was fair.

First, the purpose and character of the issue were transformative, favoring a fair use finding. The "transformativeness" inquiry asks whether the new use "merely supersedes the object of the original creation or adds some new purpose or character." When and whether a use is deemed transformative often poses a difficult question because the use can be viewed from different perspectives. From one perspective, the reader of a cached copy of Field's (putative) poetry might be deemed to be making the same use as the reader of the original work, *viz.*, to enrich their lives with the aesthetic. Field's "works" were not such as to compel such a perspective, and the court chose to focus instead on the functional characteristics of cached works as a class, rather than the claimed poetical characteristics of these particular works.

The court identified five respects that distinguished cached versions or links from the originals and that indicate they do not merely supersede the uses of the original works.

1. Google's cache functionality allowed access to content when the original work was inaccessible. "In these circumstances, Google's archival copy . . . obviously does not substitute for the original."
2. Cached links allow internet users to monitor and compare changes in web pages over time.
3. Cached links allow users to understand why a page was responsive to their original query, and therefore facilitate effective searching.
4. The cached links are less prominent than the links to the original works, which are also always displayed by Google, thereby rendering a substitution effect unlikely.
5. Site owners can readily disable the cache functionality; the fact that owners of billions of web pages have not done so is strong evidence they do not view Google's caches as substitutes for their original works.

"Google serves different and socially important purposes in offering access to copyrighted works through 'Cached' links and does not merely supersede the objectives of the original creations," therefore copying and distribution of Field's pages was transformative.

The "commercial" character of Google as an enterprise did not negate the fair use conclusion regarding the first factor because Field's works were among billions similarly stored and because Google displayed no advertising on the cached pages.

The second factor, the *nature of the copyrighted work*, only slightly favored Field. Although the court presumed that Field's works were creative in character, the fact that they were published and available for free, and that Field deliberately enabled searching for these pages, militated somewhat against fair use.

Third, the *amount and substantiality of the use*, while total, also did not weigh against fair use where, as here, the new use serves a different function from the original and the original was available for free, particularly because the transformative purposes could not be achieved by less than complete copying. This factor was therefore neutral.

Fourth, regarding the *effect of the use on the market for or value of the copyrighted work*, there was no evidence of any market for or harm to any market for cached copies, and there was evidence of the near-universal industry acceptance of uncompensated caching. This factor therefore strongly favored fair use.

Finally, the court considered, as an additional factor, *Google's good faith in operating its system cache*, which favored fair use. Google observed industry-standard protocols and assisted site owners in preventing caching should they wish to do so; Google promptly removed Field's pages from its cache on learning of his objection; and Field's bad faith added further weight to the "good faith" factor in Google's favor.

Considering all the factors together, the district court held Google's use to be fair as a matter of law.

DMCA Safe Harbor. Finally, on cross-motions for summary judgment, the court held that Google qualified for the caching safe harbor of 17 U.S.C. § 512(b). First, caching information as Google does for 14 to 20 days satisfies the requirement that cached copies for "intermediate and temporary." Second, the transmission of the material from Field to Google itself meets the requirement of § 512(b)(1)(B) that material be transmitted from a person other than the one who makes it available at the direction of the other person. Finally, Google's caching satisfies the requirement that its 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]."

On all of these multiple grounds, the court therefore granted summary judgment to Google and against Field.

Fair Use & Peer-to-Peer "Sampling"; Statutory Damages & the Jury Right

BMG Music v. Gonzalez, 430 F.3d 888 (7th Cir. 2005)

A number of prominent copyright cases have in recent years considered the secondary liability of providers of peer-to-peer technologies and services used for the unauthorized distribution of music and other copyrighted matter. In this case, the district court and the Seventh Circuit considered instead the liability of an individual user of such services.

Cecilia Gonzalez used KaZaA to download more than 1,370 copyrighted songs to her computer over a period of a few weeks. She claimed to have already owned CDs containing some of these songs, and subsequently to have purchased others after sampling the music, but conceded that she never owned purchased copies of 30 songs. On BMG Music's motion for summary judgment, Gonzalez was held liable for copyright infringement based on those 30 copies and BMG was awarded $22,500 in damages – 30 times the low end of the $750-to-$30,000-per-infringed-work statutory damages range.

The case posed two issues: whether Gonzalez' uses of these works was fair; and whether she was entitled to a jury trial on statutory damages.

Fair use. The Seventh Circuit affirmed summary judgment that Gonzalez' copying of the 30 songs was not fair use. "Gonzalez was not engaged in a nonprofit use; she downloaded (and kept) whole copyrighted songs (for which, as with poetry, copying of more than a couplet or two is deemed excessive); and she did this despite the fact that these works often are sold per song as well as per album. This leads her to concentrate on the fourth consideration: 'the effect of the use upon the potential market for or value of the copyrighted work.' [¶] As she tells the tale, downloading on a try-before-you-buy basis is good advertising for copyright proprietors, expanding the value of their inventory." 430 F.3d at 890.

The Seventh Circuit did not buy the tale, it held, because many users are bound to keep the downloaded files without buying originals, because the authors and publishers are entitled to control the means by which their works are promoted (and to collect revenue from them if they so choose), and because copyright owners do derive revenue from such established means of introducing music to new audiences as radio broadcast, internet streaming, and licensed use of limited, partial samples. "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 . . . ." 430 F.3d at 891.

Statutory Damages. BMG sought only the minimum statutory damages required under the statute – $750 per copy since Gonzalez was not entitled to an innocent infringer defense – and the district court awarded that amount on summary judgment. Gonzalez maintained she was entitled to a jury trial on the amount of statutory damages. Not so, held the Seventh Circuit. "If BMG Music had requested more than $750 per work, then Gonzalez would have been entitled to a trial. . . . What number between $750 and $30,000 is 'just' recompense is a question for the jury, unless both parties agree to decision by the court." But there is no question for the jury as to the amount when the copyright holder seeks only the statutory minimum; arguing otherwise amounts to claiming a right to have the jury nullify the statutory damages award.

Computer Maintenance Competition Assurance Act (17 U.S.C. § 117(c))

Storage Technology v. Custom Hardware Engineering, 421 F.3d 1307, *further opinion on denial of petition for rehearing* 431 F.3d 1374 (Fed. Cir. 2005) [2]

In this case, a divided panel of the Federal Circuit weakened the position of software copyright owners by reading expansively the right to copy that 17 U.S.C. § 117(c) gives independent service operators, and reading narrowly an express contractual term that sought to preclude other-party use of plaintiff's maintenance program.

The plaintiff in the Federal Circuit's *StorageTek* case sold large data storage systems comprised of automated tape cartridge libraries and computers and software that ran the libraries and the overall system. "Maintenance Code" software was pre-loaded on the systems, but was not licensed to the purchasers – indeed, the license for plaintiff's other software for the storage system expressly provided that the purchaser acquired no rights to use the maintenance code. The Maintenance Code booted up automatically when the system was turned on, but the program and its diagnostic data were protected by a password scheme that kept anyone but StorageTek maintenance employees from accessing and using Maintenance Code.

Defendant Custom Hardware Engineering ("CHE") was an independent service organization in competition with StorageTek for the business of servicing StorageTek systems. CHE circumvented the password protection measures, then used the diagnostic data generated by the Maintenance Code in order to provide maintenance for the StorageTek systems.

StorageTek sued CHE, alleging that CHE infringed StorageTek's Maintenance Code copyrights when it booted up the system for servicing (thereby making a copy of the software in RAM), that CHE violated the DMCA when it circumvented StorageTek's password protection, and that CHE breached StorageTek's trade secrets in the fault codes that carried diagnostic information about the system when it used them for servicing.

The Federal Circuit rejected the copyright infringement claim on two grounds: first, that CHE was entitled to create the RAM copy under the Computer Maintenance Competition Assurance Act (codified at 17 U.S.C. § 117(c)); and second, that CHE was impliedly licensed to make the copy under StorageTek's agreements with the purchasers of the systems.

The § 117(c) Defense to RAM Copying. Section § 117(c) provides it is not an infringement for one authorized by the owner of a machine to make a copy of a computer program, if it is made "solely by virtue of activation of a machine . . . for purposes only of maintenance or repair of that machine." The defense under § 117(c) is subject to two further conditions: (1) that the new copy, created as a result of activating the machine, "is used in no other manner and is destroyed immediately after the maintenance or repair is completed; and (2) 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 Federal Circuit rejected StorageTek's arguments that CHE was not shielded from liability by § 117(c).

StorageTek contended that CHE's activities did not comport with either proviso of § 117(c). First, StorageTek argued that CHE was not eligible under § 117(c) because CHE did not – as required by § 117(c) condition (1) – destroy the copy of the Maintenance Code "immediately" after completion of repair or maintenance; indeed, the copy of Maintenance Code that CHE used was kept in RAM for the entire period of CHE's service contract. But "maintenance," the Federal Circuit held, is a continuous process that includes ongoing monitoring of system performance. Destruction of the RAM copy at the conclusion of the service contract was therefore "immediate" enough, and the copy did not need to be destroyed before then.

StorageTek also maintained that CHE's use of the diagnostic Machine Code was inconsistent with condition (2) of § 117(c). This provides that if a copy is made of "any computer program or part thereof that is not necessary" for the machine to be activated, it may "not [be] accessed or used other than to make such new copy by virtue of the [machine's] activation." StorageTek argued that since the Maintenance Code's functions were diagnostic and maintenance-oriented in nature, the Maintenance Code was not necessary for the machine to be activated. Since CHE did access and use the fault symptom codes generated by the maintenance software in order to perform system maintenance, it was disqualified from the benefit of § 117(c).

The *StorageTek* majority acknowledged that accessing freestanding diagnostic programs would violate the condition set forth in § 117(c)(2), making the defense unavailable. This conclusion was unavoidable in light of the legislative history, never referred to by the court, which specifically uses maintenance programs as examples of programs not necessary for machine activation. Notwithstanding, the court held, because the Maintenance Code and what it called the "functional code" that operated the storage system were thoroughly entangled, loading the Maintenance Code into RAM was "necessary" to activate the machine, and condition (2) did not consequently bar the § 117(c) defense.

The Federal Circuit's convoluted argument never actually explained why "entanglement" should make a program – or, as the statute provides, a "part thereof" – necessary for machine activation within the meaning of the statute. That the disputed application program is configured to actually launch when the system boots up, creating a RAM copy, can scarcely be sufficient to show that a program is "necessary" for machine activation. If that were the case, copies created "by virtue of activation" of a computer would always be "necessary," and condition (2) could never come into play. Further, condition (2) of § 117(c) specifically anticipates situations in which "*part*" of a program may not be necessary for machine activation (and bars accessing or using that part if the defense is to apply). No matter how interwoven the different parts of the code might be, consequently, the statute obviously contemplates that in the end we consider whether there is a part of the program that boots up which is not

necessary for machine activation, and whether the defendant is accessing or using that part. In this case, whether entangled with functional code or not, the part of the code performing maintenance functions was not necessary for machine activation, so – under condition (2) – CHE could not use that part of the program and still be shielded from the infringement claim. CHE did so, therefore § 117(c) should not have protected its copying.

The Federal Circuit also ignored the point that condition (1) of § 117(c) makes the defense unavailable unless the new copy created by machine activation is used in "no other manner" than machine activation. CHE did use the copy in another manner, viz., to obtain information (diagnostic fault messages) it used to maintain the StorageTek systems. It was therefore not entitled to make a copy of Maintenance Code under the terms of § 117(c).

In its December 2005 opinion, the panel (divided as in the original decision) offered "a brief additional discussion" on the § 117(c) issue. Again, the panel asserted that "determining whether a particular piece of software is 'necessary for [the] machine to be activated' is not a simple task." Since, the court reasoned, the part of the code that was required to boot up the machine was intertwined with the maintenance code, even if the maintenance code could later be deactivated, this "does not change the fact that a copy of the entire maintenance code must be loaded into RAM when the machine is turned on."

The court's additional discussion remains as flawed as its original treatment of this issue. First, again, that a part of the code was in fact loaded when the machine was activated does not mean that that part was *necessary* for machine activation. Second, the court ignores § 117(c)'s requirement in condition (1) that "such new copy" (the copy "made solely by virtue of activation" of the computer) be "*used in no other manner* . . . ." CHE's manner of use of the maintenance code went beyond its inevitable creation when the StorageTek system was activated; CHE used the code thereafter for maintaining the system. Regardless of whether the initial making of the copy was privileged under § 117(c), consequently, CHE's subsequent exploitation of that copy breached § 117(c)'s clear requirement that independent service providers not use a copied program except to activate the machine.

The Federal Circuit's Implied License Ruling. In an equally strained alternative holding, the Federal Circuit also found that, notwithstanding contract language that specifically excludes use of the maintenance code, purchasers were entitled both to load the code and to authorize others to use it. Nonetheless, the majority concluded that because the code would be copied automatically when the machine was turned on, equipment owners were necessarily authorized to use the code.

Various provisions of the agreement, the court argued, implied that "the license is tied to the piece of equipment on which the software resides." The court pointed, for example, to a provision that owners of the equipment "'may transfer possession of Internal Code only with the transfer of the Equipment on which its use is authorized,'" and the court also noted that the

"license grants the customer the use of the code for 'the sole purpose of enabling the specific unit of Equipment for which the Internal Code was provided.'" But the fact that the license and equipment are "tied," for some stated purposes, simply does not imply that anyone starting up the machine – even if impliedly authorized to load the Maintenance Code into RAM as part of the start-up process – was authorized to *use* that code in order to perform maintenance. Any such implication is also negated by the fact that there was no license to the Maintenance Code to be tied to the equipment. The StorageTek software license (not quoted in the decision) expressly provided that it "confers [on the purchaser of the storage system] *no license or other right to use Maintenance Code*." (Pet. for Rehearing at 10.) It is difficult to square the purported implied license granting a right to use with the express contractual negation of any such right.

Responding to the court's analysis that tied the Internal Code license to the equipment, StorageTek's rehearing petition pointed out that the license's definition of "Internal Code" excluded Maintenance Code. The court dealt with this through denial: "Our decision [the December 2005 opinion states] did not rest on an interpretation of the term 'Internal Code,' but rested instead on our conclusion that permission to copy StorageTek's software was implicit in the licensing agreement, which permits the licensee to activate the equipment." The argument is disingenuous because the panel plainly *had* relied on the provisions concerning Internal Code as the basis for its analysis that an implied license was tied to the equipment. Second, again, the asserted implied authorization to create a copy of Maintenance Code by activating the equipment is an entirely different matter from any implied contractual right to *use* or authorize another to *use* that code, especially in the face of an express provision to the contrary.

The key lesson of the *StorageTek* contract analysis would seem to be that software owners' license agreements must be extraordinarily explicit about the point if they want to bar third-party use. This is a disturbing conclusion because – up to this decision – few readers would have found much ambiguity in a license including the language employed by StorageTek with regard to its Maintenance Code.

Looking at the big picture under § 117(c), the Federal Circuit seems to have missed the point. Section § 117(c) was intended to prevent computer system manufacturers from leveraging their system software copyrights into monopolies on maintenance services, merely because their maintenance programs loaded automatically when the systems booted up. That is, independent service providers should not be considered infringers just because they unavoidably copied a program without authorization when that program automatically launched at system startup. But the fundamental issue in *StorageTek* was not whether CHE could merely turn on the StorageTek machines in order to service them. The issue was whether CHE was entitled to a free ride – to *use* StorageTek's maintenance program to provide maintenance services rather than developing and using its own program. Particularly in light of

the legislative history indicating Congress's intent *not* to allow independent service operators to actually use copyright holders' maintenance programs, the policy reason for the outcome is hard to fathom.

The Circumvention and Trade Secret Claims. The Federal Circuit disposed of the two remaining issues, StorageTek's circumvention claim and its trade secrets claim.

In its holding in a 2004 case, *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 381 F.3d 1178, the Federal Circuit had held that circumventing an access-controlling technological protection measure was only unlawful if the circumvention "infringes or facilitates infringing a right protected by the Copyright Act." Since the court had concluded in *StorageTek* that CHE's copying was protected by § 117(c), CHE could not be liable for circumvention. The ruling confirms an important point: Although a number of other courts have held to the contrary, under *Chamberlain* and *StorageTek*, defenses to the underlying copyright infringement are defenses to circumvention claims. If this is the case for the § 117(c) defense, there would be no apparent reason to treat fair use or any other defense differently.

Finally, regarding the trade secret claim, the court held there was no violation because (1) the fault symptom codes generated by StorageTek's Maintenance Code had themselves not previously been kept secret, and (2) the reasons a particular machine no longer owned by StorageTek is malfunctioning cannot be a secret.

DIGITAL MILLENIUM COPYRIGHT ACT

Circumvention Bar & Non-Infringing Alternative Services

Davidson & Associates v. Jung, 422 F.3d 630 (8th Cir. 2005)

In this case, the Eighth Circuit strengthened the hand of software owners, interpreting the Digital Millennium Copyright Act's circumvention bar expansively and upholding a contractual prohibition on reverse engineering against a preemption challenge.

Plaintiff Davidson & Associates (referred to by its dba "Blizzard") developed computer games that could be played in an online multi-player manner when in "Battle.net mode," using Blizzard's Battle.net servers. To prevent infringing copies of Blizzard games from being played at Battle.net, purchasers of authentic copies were required to enter a "CD Key" that was printed on a sticker attached to the product packaging. Based on this code, the games initiated an authentication sequence or "secret handshake" with the Battle.net server before online gaming was permitted.
The outside packaging of nearly all Blizzard games displayed a notice that the game and service were subject to an end-user license agreement (EULA) and Terms of Use (TOU). Before

installing a copy of a Blizzard game, a purchaser was required to select and click on a button marked "I agree," manifesting acceptance of the EULA and TOU. The EULA prohibited reverse engineering and the TOU barred users from engaging in emulation or from hosting or providing "matchmaking" services for Blizzard games.

Defendants developed, apparently on a non-commercial basis, an alternative online gaming environment for the Blizzard games, designed to emulate Battle.net but hosted on defendants' own server at bnetd.org. In order to do so, defendants (who had previously agreed to the EULA and TOU) reverse engineered Blizzard's games to learn how to use their protocol language, modified the computer file that directed players to Battle.net, and created the Battle.net-emulating bnetd.org server on which they provided matchmaking services for multi-player game play. But unlike Battle.net, bnetd.org did not determine whether a CD Key was valid or already in use before allowing access to Battle.net mode, and therefore did not prevent infringing copies of Blizzard games from being played online.

Blizzard sued for copyright and trademark infringement, breach of contract and unlawful circumvention. The copyright and trademark claims were resolved pursuant to a consent decree and permanent injunction whereby the defendants would transfer the bnetd.org domain name to Blizzard, would be enjoined from participating in future efforts to develop any emulators for Blizzard games, and would face no liability for monetary relief on any claim. The existence of the consent decree is mentioned in the district court and appellate opinions, but its terms are not recited and seem to play no role in the analysis.

Blizzard won summary judgment on the remaining claims, for breach of the EULA and TOU and for unlawful circumvention. The Eighth Circuit affirmed in an opinion so confusing and cryptic at points as to border on incoherence. Below, we summarize the outcomes and attempt to extract possible "holdings" from the decision.

Regarding the EULA – TOU contract claims. *Davidson* stands for two propositions:

- EULAs and TOUs are enforceable contracts when assent is manifested through click-on license agreements.
- A contractual prohibition against reverse engineering is enforceable against the defense that reverse engineering contract provisions are "preempted" by the Copyright Act.

Regarding the DMCA Circumvention claim. In a particularly confusing part of its opinion, the Eight Circuit determined that the bnetd.org server and emulator were a circumventing technology under 17 U.S.C. § 1201(a)(2) (which deals with access controls), and that the reverse engineering defense under § 1201(f) did not apply.

The court does not state what was being protected from unauthorized access by the technological protection measure, and the prima facie violation is not clear. The totality of the Eighth Circuit's explanation: "The bnetd.org emulator had limited commercial purpose because its sole purpose was to avoid the limitations of Battle.net. There is no genuine issue of material fact that Appellants designed and developed the bnetd.org server and emulator for the purpose of circumventing Blizzard's technological measures controlling access to Battle.net and the Blizzard games."

CD Key, the secret handshake and the protocols that prevented unauthorized access to Battle.net appear to constitute effective technological measures entitled to protection against circumvention. But they prevented unauthorized access to Battle.net, and the defendants did not bypass these measures to engage in or facilitate unauthorized (or any other) access to Battle.net. Rather, they afforded access to their own, emulating server, which offered comparable functionality. Similarly, as far as can be discerned from the court's opinion, the CD Key does not control access to the Blizzard game itself (as opposed to controlling a game's access to a server for purposes of multi-player play), and it does not appear that defendants circumvented an access control (if any there be) for the game. Interpreting broadly, and without the benefit of much analysis by the court, the Eighth Circuit was arguably holding:

- When a party provides access to a non-infringing, emulating server as an alternative to a server protected by the publisher's access controls, this constitutes "circumvention" of the access controls employed by the publisher's server.

The reverse engineering defense. The court rebuffed defendants' "reverse engineering" defense under § 1201(f)(1). This section exempts a circumventor from liability when the circumvention's "sole purpose [is] identifying and analyzing those elements of [a] program that are necessary to achieve interoperability of an independently created computer program . . . to the extent any such acts of identification do not constitute [copyright] infringement under this title [Title 17]."

The wording of the statute is confusing, and it is not clear how "acts of identification" of elements necessary for interoperability could ever themselves constitute copyright infringement. Interestingly, when the Eighth Circuit summarized the requirements of the statute, it stated the condition as that "the *alleged circumvention* did not constitute infringement." (2005 U.S. App. Lexis 18973 at *30, emphasis added.)

Presumably, this was the basis of the court's rejection of the reverse engineering defense: Immediately after reciting the requirements of § 1201(f)(1), the Eighth Circuit simply stated: "Appellants' circumvention in this case constitutes infringement." By way of explanation, the court alluded to the fact that defendants' bnetd.org server allowed Blizzard game users to access Battle.net mode features and to play with other gamers on the bnetd.org server

regardless of whether they had a valid CD key, with the result that unauthorized copies of Blizzard games could be and were freely played on bnetd.org servers.

But what was the infringement? Making a server available for the exchange of game data among Blizzard players (some of whom use infringing copies) would not appear to constitute direct copyright infringement by defendants. Neither would such actions appear to constitute contributory infringement. That requires proof of (1) an underlying direct infringement, to which (2) the defendant materially contributes (3) with knowledge of the direct infringement. In *Davidson*, the defendants knew that unauthorized and presumptively infringing copies had been made and that they were being used in conjunction with bnetd.org. But since defendants did not apparently participate, directly or otherwise, in the creation of any "pirated" copies of Blizzard games, their actions would not ordinarily be said to "materially contribute" to an infringing act. Although the Eighth Circuit does not trouble to play out the analysis, the following theories might explain the outcome:

- Circumvention defendants are not entitled to the reverse engineering defense of § 1201(f) if their reverse engineering allows a direct infringer to use his infringing copy interoperably with the defendants' independently created program.

- The "non-infringement" requirement of the § 1201(f)(1) defense is violated by acts that would make a party secondarily liable as well as by direct infringement. Each time an unauthorized copy of a Blizzard game is launched, a new infringing copy is made in the RAM of the infringer's computer. The defendants – by offering an otherwise unavailable service to the infringer at that time – provided an incentive for the creation of the infringing RAM copy and facilitated the Battle.net mode use of that copy. Hence, they should be deemed (contributory) infringers.

The first point is suggestive of "accessory after the fact" liability, not secondary liability under copyright. The second point evokes the new "inducement of infringement" doctrine, but without meeting the high standard for copyright inducement set forth by the Supreme Court in *MGM v. Grokster*.

Conclusion. Although the reasoning of this case is not especially satisfying, the outcomes is clear enough. The Eighth Circuit expanded the sweep of the anti-circumvention provisions of the DMCA by treating "circumvention" broadly and by interpreting the reverse engineering defense narrowly, to the benefit of copyright holders who employ technological protection measures. We doubt the case is the last word on the subject.

Password-Use & Circumvention

Egilman v. Keller & Heckman, LLP, 401 F.Supp.2d 105, 2005 U.S. Dist. Lexis 28245* (D.D.C. 2005)

The DMCA bars circumvention of technological measures that effectively control access to copyright-protected works. The Act states:

> "[T]o 'circumvent a technological measure' means 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."

17 U.S.C. § 1201(a)(1)(A).

"Descrambling" and "decrypting" are relatively clear concepts, but what does it mean to "avoid" or "bypass" a technological protection measure ("TPM")? A recent decision of the District Court for the District of Columbia affirmed the conclusion of a 2004 Southern District of New York case holding that unauthorized use of a valid password to gain access to a web site not open to the general public does not constitution circumvention within the meaning of the DMCA. *Egilman* at *17, citing *I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F.Supp.2d 521, 532-33 (S.D.N.Y. 2004).

In *Egilman*, the plaintiff operated a personal web site accessible to his students and others possessing a valid user name and password. When the defendant allegedly misappropriated information by employing a correct password not properly issued to him, among other claims the plaintiff asserted a cause of action under the DMCA, 17 U.S.C. § 1201(a)(1)(A), alleging that the defendant had circumvented a technological security measure that effectively controlled access to a copyrighted work. The district court denied the claim on a motion for judgment on the pleadings.

Egilman accepted the reasoning of *I.M.S.* that "what defendant avoided and bypassed was *permission* to engage and move through the technological measure," and that defendant did not avoid or bypass the measure in its technological character. As the *Egilman* court itself explained,

"What is missing from this statutory definition [the one quoted above] is any reference to 'use' of a technological measure without the authority of the copyright owner, and the court declines to manufacture such language now. . . . [U]sing a username/password combination as intended – by entering a valid username and password, albeit without authorization – does not constitute circumvention under the DMCA." *Id*. at *20.

The *Egilman* court also declined to distinguish *I.M.S.* on the basis that in *I.M.S.* the defendant had purloined a password legitimately issued to a third party, whereas there was no such allegation in *Egilman*.

The *Egilman* decision does not mention the point, but the motion papers make clear that the defendants in *Egilman* claimed to have "guessed" the correct username and password. Quere whether it should make a differenceto the outcome had the "guessing" consisted of using a password-cracking program that rapidly generated candidate alphanumerical combinations until the correct password was automatically "guessed."
In the view of the district court that would apparently not matter: "It was irrelevant who provided the username/ password combination to the defendant, or, given that the combination itself was legitimate, how it was obtained." *Id*. at *21.

It is entirely possible that another court would regard an automated, computerized means of guessing as a method of "bypassing" a TPM within the meaning of the statute, particularly because the line between "using" a technological measure and avoiding, bypassing or impairing it may not turn out to be so clear in every case, and it is not self-evidence whether "circumvention" should be deemed to require overcoming resistance or avoidance by the TPM.

Copyright Management Information

The IQ Group, Ltd. v. Wiesner, 409 F.Supp.2d 587 (D.N.J. 2006)

In some respects, *The IQ Group* poses a similar question to that in *Egilman*, namely, the extent to which the DMCA is limited to high-technology attacks or systems.

Another section of the DMCA, 17 U.S.C. § 1202, bars alteration or removal of "copyright management information" ("CMI"), which is defined *inter alia* as "the name of, and other identifying information about, the author of a work" or "the copyright owner of the work," as well as "identifying numbers or symbols referring to such information or links to such information." § 1202(c).

Plaintiff The IQ Group prepared email advertisements that included an IQ logo as well as a hyperlink which, when clicked, directed the user to a page on IQ's web site that allegedly contained copyright notices. Defendants distributed the same ads, but removed the IQ logo and hyperlink. Since the logo was an identifying symbol, and the hyperlink led to identifying information about the copyright holder, IQ alleged (among other claims) that removal of these items represented a CMI violation.

The IQ Logo and the Trademark–Copyright Interface. The district court concluded that a construction that allowed a logo, which functions as a service mark, to be treated as CMI would essentially turn trademark claims into DMCA claims, creating "a species of mutant trademark/

copyright law, [and] blurring the boundaries between the law of trademarks and that of copyright." The court declined to so extend and blur copyright and trademark law.

The Intended Technological Character of CMI Protection. Although, the court acknowledged, the statutory definition of CMI was quite broad, the court held, in this case of first impression, that the legislative history and other sources indicated that a narrower interpretation was appropriate. Particularly in light of the goals of the DMCA, taken as a whole, of facilitating electronic and internet commerce, and of maintaining the integrity of the electronic marketplace by preventing fraud and misinformation, the district court held that § 1202 "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." 409 F.Supp.2d at 597.

Based on this construction of the statute, the court granted defendant's motion for summary judgment as to violations of § 1202:

> "Although the advertisements were sent via email, and thus likely copied and distributed as part of an automated process within a computer network environment, this does not bring the information removal within *§ 1202*. To come within *§ 1202*, the information removed must function as a component of an automated copyright protection or management system. IQ has not alleged that the logo or the hyperlink were intended to serve such a function. . . . There is no evidence that IQ intended that an automated system would use the logo or hyperlink to manage copyrights, nor that the logo or hyperlink performed such a function, nor that Wiesner's actions otherwise impeded or circumvented the effective functioning of an automated copyright protection system." *Id*.

Conclusion

It would be difficult to discern a strong trend in the copyright and DMCA cases over the last year, tending either to favor or limit the interests of copyright holders as opposed to users of copyright-protected works or competitors. Many of the cases are part of the ongoing process of consolidation of our understanding of governing legal principles, a process which is clearly not yet concluded. Stay tuned for 2006-07 and beyond!

---

[1] The author's firm represents Google in various matters, although not in the cases discussed herein in which Google was a party.

[2] The author and his firm represent Sun Microsystems, which recently acquired Storage Technology, the plaintiff in this case.

www.fenwick.com

Lawyers who get IT.™