FENWICK & WEST LLP
Silicon Valley Center • 801 California Street • Mountain View, CA 94041
Tel 650.988.8500 • Fax 650.938.5200 • www.fenwick.com

EDiscovery:

copyright © Western Digital Corporation

Preserving, Requesting & Producing Electronic Information

by:

Lisa M. Arent

Robert D. Brownstone

William A. Fenwick

© Copyright 1999, 2002, 2003
Lisa M. Arent and Fenwick & West LLP

6/11/03 updated version by Robert D. Brownstone

Hard copy of 12/5/02 version available at:
19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 131 (Dec. 2002)

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

CONSTITUTIONS, STATUTES, RULES & REGULATIONS

FEDERAL

TABLE OF AUTHORITIES
(continued)

Page(s)

STATES

ARTICLES, BOOKS, GUIDES AND COMPILATIONS

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

PROVIDERS OF SERVICES & PRODUCTS

I. INTRODUCTION[1]

As one federal judge so astutely predicted two decades ago:

> It may well be that Judge Charles E. Clark and the framers of the Federal Rules of Civil Procedure could not foresee the computer age. However, we know we now live in an era when much of the data which our society desires to retain is stored in computer discs. This process will escalate in years to come; we suspect that by the year 2000 *virtually all data will be stored in some form of computer memory*.[2]

The 1980 prediction was not too far off. In our high-tech era, a body of law[3] has evolved regarding the parameters of the preservation, collection, and production of

---

[1] The authors wish to thank Michelle van Wiggeren and Steve Goldberg for their invaluable help in updating and revising the predecessor of this paper, "*Professionalism in CyberDiscovery; The Proper Course for Retaining and Producing Electronic Documents*," originally written and copyrighted in 1999 by Lisa M. Arent. The authors also wish to thank Rachael Samberg and Leslie Morris for their help in the Spring 2003 updating of this paper.

[2] *National Union Elec. Corp. v. Matsushita Elec. Indus. Co.*, 494 F. Supp. 1257, 1262 (E.D. Pa. 1980) (emphasis added). Only .003% of the unique information produced annually by the world is in printed documents. A study, titled *"How Much Information"* and published in 2000, by the faculty and students at the School of Information Management and Systems at the University of California at Berkeley reported:

> The world produces between 1 and 2 exabytes of unique information per year, which is roughly 250 megabytes for every man, woman, and child on earth. An exabyte is a billion gigabytes, or 1018 bytes. Printed documents of all kinds comprise only .003% of the total. Magnetic storage is by far the largest medium for storing information and is the most rapidly growing, with shipped hard drive capacity doubling every year. Magnetic storage is rapidly becoming the universal medium for information storage.

Peter Lyman & Hal R. Varian, "How Much Information" (2000). <http://www.sims.berkeley.edu/research/projects/how-much-info/>.

[3] An excellent and up-to-date compilation ("organized [both] by jurisdiction and by topic") of electronic discovery case blurbs is maintained by OnTrack Data International <http://www.krollontrack.com/> at its "Case Law List" page <http://www.krollontrack.com/LawLibrary/CaselawList/>. A new key resource is the working draft of *"THE SEDONA PRINCIPLES: Best Practices, Recommendations & Principles for Addressing Electronic Document Production"* (Mar. 2003), available, along with its accompanying *"Observations on 'The Sedona Principles',"* (Apr. 2003) at <http://www.thesedonaconference.org/publications_html>. Other helpful sources are Applied Discovery's "Law Library" <http://www.applieddiscovery.com/lawLibrary/default.asp>; New Technology Inc.'s (NTI's) "Computer Forensics for Civil Litigation: Recent Articles from the Legal Press" <http://www.dataforensics.com/articles.html>; CoreFacts' "Electronic Discovery" case list at <http://www.corefacts.net/electronicdiscovery/electronicdiscovery_main.htm>; and, though not as up-to-date, the "Library - Digital Discovery" <http://cyber.law.harvard.edu/digitaldiscovery/library.html>posted by Harvard Law School's Berkman Center for Internet & Society on October 10, 2000.

electronic evidence.[4] This paper discusses the application of discovery rules and common law discovery principles to electronic information issues.

II. PRESERVATION AND COLLECTION OF ELECTRONIC DATA

A. The Duty to Preserve Evidence

1. Preservation Obligations in the Electronic Context

A party has a duty to preserve potentially relevant evidence. Evidence includes all forms of information: not only hardcopy documents,[5] but also electronic information stored on a computer, in a database or in any other electronic format. A requesting party is entitled to obtain discoverable information from an electronic source to the same extent as from a filing cabinet.[6] In each situation, the responding party must determine the potential sources and locations of responsive information and then conduct a diligent search for responsive materials.

Rule 34 of the Federal Rules of Civil Procedure defines the term "document" broadly, to include information in any tangible format.[7] Although discovery of electronic data has become an issue of increased interest and concern over the last several years, the notion that computer data is discoverable is not new. In 1970, Congress modified Rule

---

[4] "The U.S. market for electronic discovery services is 'probably a couple billion dollars' in the near term . . . and in the next three to four years . . . will probably grow to 'several billion dollars,' with the international market adding another 25 to 50 percent," according to the associate director of a $10 billion venture capital firm that invested in a provider of electronic services to law firms. Aliza Earnshaw, "*Fios Investors See Big Market For Local Firm*," The Business Journal Portland (July 20, 2001). <http://portland.bizjournals.com/portland/stories/2001/07/23/story6.html>

[5] The older discovery terminology "document" is confusing and misleading in the current world, where the vast majority of information is electronic and is never contained in documents. Courts and parties can be misled by references to documents when discussing relevance, admissibility, the duty to preserve and the obligation to produce. Litigants' and potential litigants' obligations relate to *information*. Thus, it would be desirable to have the procedural rules refer to "information" requests rather than "document" requests.

[6] *Linnen v. A.H. Robins Co.,* 10 Mass. L. Rptr. 189 (Super. Ct. 1999). See also *Jones v. Goord*, 2002 U.S. Dist. LEXIS 8707, *17 (S.D.N.Y. May 16, 2002) (discoverability's legal "framework applies to requests for electronic or computer-based information just as it applies to more traditional materials. 8A Charles Alan Wright & Arthur R. Miller, Federal Practice and Procedure, § 2218 at 451 (2d ed. 1994)."), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/linnen.html>.

[7] Fed. R. Civ. P. 34(a) encompasses "documents (including writings, drawings, graphs, charts, photographs, phonorecords, and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form)." Rule 34 also enables a party to seek "to inspect and copy, test, or sample any tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served."

34 to explicate that the term "documents" encompassed more than just hardcopies.[8]

Neither of the California Discovery Act provisions regarding the production of "documents and tangible things" defines "document."[9] Instead, in all Discovery Act sections, by virtue of Cal. Code Civ. Proc. § 2016(b)(3), "document" is coextensive with "writing" as defined in California Evidence Code § 250. Section 250 defines "writing" as "handwriting, typewriting, printing, photostating, photographing, and every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof." That definition has been interpreted broadly to include information in electronic form. [10]

The broad definition of "documents" typically used in requests for production encompasses information stored on computers and on computer media, such as floppy disks, zip drives, jaz drives,[11] and archival/emergency storage devices (such as back-up tapes).[12] Moreover, electronic versions of documents can contain additional, non-printed/hidden information (known as metadata), such as the dates of creation, access

---

[8] The 1970 Advisory Committee Notes provide that Rule 34 encompasses "electronic data compilations from which information can be obtained only with the use of detection devices." "[W]hen the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into usable form." *Id*. "[C]ourts have ample power under Rule 26(c) to protect respondent against undue burden or expense, either by restricting discovery or requiring that the discovering party pay costs. [I]f the discovering party needs to check the electronic source itself, the court may protect respondent with respect to preservation of his records, confidentiality of nondiscoverable matters, and costs." *Id*. *See generally* Hon. Shira A. Scheindlin & Jeffrey Rabkin, "*Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task*?" 41 B.C. L. REV. 327 (2000). <http://www.bc.edu/schools/law/lawreviews/meta-elements/journals/bclawr/41_2/03_FMS.htm>. Cf. SEC Rule 17a-4, 17 C.F.R. § 240.17a-4 ("Electronic Storage of Broker-Dealer Records"). *See also* footnote 193 below.

[9] Cal. Code Civ. Proc. § 2031 (inspection and copying of documents and tangible things in possession, custody, or control of another party to the action); Cal. Code Civ. Proc. § 2020 (inspection and copying of nonparty's documents and tangible things).

[10] *Aguimatang v. California State Lottery*, 234 Cal. App. 3d 769, 798, 286 Cal. Rptr. 57 (1991) (computer's magnetic tapes constituted "writing" under § 250). *See also* Michael R. Overly, "Overly on Electronic Evidence in California," § 3.05[A] (West Group 1999).

[11] A "Jaz drive" is "a removable disk drive" developed by Iomega Corporation. It "holds up to 2 GB of data. The fast data rates and large storage capacity make it a viable alternative for backup storage as well as everyday use." "Jaz Drive." <http://www.pcwebopedia.com/TERM/J/Jaz_Drive.html>

[12] *Crown Life Ins. Co. v. Craig*, 995 F.2d 1376 (7th Cir. 1993) (raw computer data constitutes discoverable documents that must be produced, even though producing party could not access the data), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/process/crownlife.html>; *R.S. Creative v. Creative Cotton, Ltd.*, 75 Cal. App. 4th 486, 489 (1999) (definition of "document" for purposes of production request "included computer tapes, discs and any information stored in a computer"); *Linnen v. A.H. Robins Co*., 10 Mass. L. Rptr. 189 (Super. Ct. 1999) ("documents" – as defined in preservation order and in subsequent document requests – encompassed data contained on back-up tapes), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/linnen.html>.

and/or modification and, if relevant, sending and receiving details.[13]

2. Nature and Consequences of Duty to Preserve

a. Introduction

The responding party's failure to preserve evidence or destruction of evidence can lead to a variety of adverse consequences. It may preclude the requesting party from obtaining otherwise relevant or discoverable evidence; it may harm the integrity of the court proceedings; and it may ultimately harm the blameworthy party.

b. Ethical Obligations

When conducting discovery, an attorney should keep in mind the principles set forth in ethics rules. Model Rule of Professional Conduct 8.4(c)-(d) proscribes "dishonesty, fraud, deceit, or misrepresentation [or] conduct that is prejudicial to the administration of justice."[14] Moreover, as to the production of evidence, Model Rule of Professional Conduct 3.4(a) provides that a lawyer shall not "unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value [; and] shall not counsel or assist another person to do any such act."[15]

c. Sanctions

Depending upon the nature of the conduct, including the degree of culpability, the ramifications in a civil litigation can include: monetary penalties (such as attorney fees, costs and/or pay-for-proof sanctions); exclusion of evidence; adverse inference jury

---

[13] *Public Citizen v. Carlin*, 184 F.3d 900, 910 (D.C. Cir. 1999) (paper printout of e-mail record not "extra copy" under 44 U.S.C. § 3301 if it does not include transmission data, such as names and addresses of recipient and author and date message sent), cert. denied, 529 U.S. 1003 (2000); *Armstrong v. EOP*, 1 F.3d 1274, 1283 (D.C. Cir. 1993) (same). One category of potentially discoverable information beyond this paper's scope is: customer identifying information maintained by Internet Service Providers ("ISP's"). *See generally Doe v. 2TheMart.com Inc.*, 140 F. Supp. 2d 1088 (W.D. Wash. 2001) (granting motion to quash subpoena; using First Amendment to reject request to reveal names of 23 individuals who posted, in online chat room, supposedly harmful messages about requesting company), *Dendrite Int'l, Inc. v. Doe No*. 3, 342 N.J. Super. 134 (N.J. App. Div. 2001) (upholding lower court ruling that corporation/defamation-plaintiff could not obtain identity of message-board-poster); and other anonymity on-line decisions linked off of the "Anonymity Online" segment of Fenwick & West's Privacy Law Resources segment of <http://www.fenwick.com>.

[14] *See also* California Rule of Professional Conduct 5-200(A) (lawyer "[s]hall employ, for the purpose of maintaining the causes confided to the member[,] such means only as are consistent with truth; [and s]hall not seek to mislead the judge, judicial officer, or jury by an artifice or false statement of fact or law").

[15] *Cf.* Model Code of Professional Responsibility DR 7-109(A) ("[a] lawyer shall not suppress any evidence that he or his client has a legal obligation to reveal or produce"); California Rule of Professional Conduct 5-220 (same).

instructions;[16] and, in an appropriately extreme case, a dismissal or default judgment.[17]

Last year, the Second Circuit analyzed the requisite "culpable state of mind,"[18] finding that "discovery sanctions, including an adverse inference instruction, may be imposed where a party has breached a discovery obligation not only through bad faith or gross negligence, but also through ordinary negligence."[19] A few months later, a Southern District of New York judge went even farther than an adverse instruction in *Metropolitan Opera Ass'n v. Local 100 Hotel Empl. & Rest. Empl. Int'l Union*, 2003 U.S. Dist. LEXIS 1077 (S.D.N.Y. Jan. 28, 2003) ("*MetOpera*"). There, the misconduct was so extreme[20] that Judge Loretta A. Preska granted "Plaintiff's motion for final "*judgment as to liability* against defendants and for . . . attorneys' fees necessitated by the discovery abuse[s] by defendants and their counsel."[21]

Drawing on her prior experience as a litigator, Judge Preska found that:

> The discovery process in this case . . . transcended the usual clashes between adversaries, sharp elbows, spitballs and even Rambo litigation tactics. This case was qualitatively different. It presented the unfortunate combination of lawyers who completely abdicated their responsibilities under the discovery rules and as officers of the court and clients who lied and, through omission and commission, failed to search for and produce documents and, indeed, destroyed evidence – all to the ultimate prejudice of the truth-seeking process.

MetOpera relied on Fed. R. Civ. P. 37, on 28 U.S. C. § 1927, and on a court's inherent

[16] See *Trigon, Inc. v. United States*, 204 F.R.D. 277 (E.D. Va. 2001) (in corporate taxpayer's refund action, finding Government's retained litigation consulting-company willfully and intentionally destroyed testifying experts' draft reports and correspondence, such that adverse inferences and other sanctions warranted); *RKI, Inc. v. Grimes*, 177 F. Supp. 2d 859, 877 (N.D. Ill. 2001) (at bench trial "[D]efendants' spoliation of evidence on their computer support[ed] a negative inference that [D]efendants destroyed evidence of misappropriation" of trade secrets; "highly suspicious" deletions and defragmentation constituted "circumstantial evidence" of misappropriation), *mot. for new trial denied*, 2002 U.S. Dist. LEXIS 7974 (N.D. Ill. May 2, 2002). Even absent formal sanctions for spoliation of evidence, at trial a party might get some mileage from an opponent's misconduct. *See, e.g., United States v. Wise*, 221 F.3d 140, 156-57 (5th Cir. 2000) (in spite of denial of requested adverse inference instruction, Defendant still could attack prosecution's failure to seize informant's computer, which then incurred data loss when informant installed new Windows '95 program), cert. denied, 532 U.S. 959 (2001).

[17] *Metropolitan Opera Ass'n v. Local 100 Hotel Empl. & Rest. Empl. Int'l Union*, 2003 U.S. Dist. LEXIS 1077 (S.D.N.Y. Jan. 28, 2003) ("Met") (granting Plaintiff's motion for judgment against labor union, union's President and union's lead organizer, in action based on allegations that union improperly involved the Met in labor dispute between union and the Met's food service provider).

[18] *Residential Funding Corp. v. DeGeorge Financial Corp*., 2002 U.S. App. LEXIS 20422, *21-22 (2d Cir. Sep. 26, 2002) (vacating jury verdict and remanding for reconsideration of whether Plaintiff's failure to timely or fully produce e-mail back-up tapes warranted adverse jury instruction).

[19] *Id.* at *4, 40.

[20] *See* the parade of horribles listed in Section II (A)(5) below.

[21] *Metropolitan Opera Ass'n v. Local 100 Hotel Empl. & Rest. Empl. Int'l Union*, 2003 U.S. Dist. LEXIS 1077, *180 (S.D.N.Y. Jan. 28, 2003) (emphasis added).

power to sanction as the justifications for the lawsuit's ultimate"result [being] driven by discovery abuse" rather than by resolution "on the merits." [22]

d. Potential Criminal Penalties

Under federal law, it is a crime to obstruct justice by "threaten[ing] or corruptly persuad[ing] another person . . . with intent to . . . cause or induce any person to alter, destroy, mutilate, or conceal an object with intent to impair the object's integrity or availability for use in an official proceeding."[23] As discussed *infra* in Section II(A)(2), a party's responsibility to preserve evidence begins when litigation can reasonably be anticipated, rather than at the moment process is served.

A fundamental misunderstanding or misconstruction of that principle has proved devastating for Arthur Andersen LLP in the now infamous Enron case. Andersen, Enron's internal and external auditor, was convicted last year on a federal obstruction/ tampering charge.[24] The criminal prosecution and a number of parallel civil lawsuits[25] were based on allegations that, while anticipating litigation, Andersen persuaded employees to shred Enron documents. "[I]n general, . . . federal prosecutors have become much tougher with companies that seek to obstruct justice since document destruction became an issue in the investigation of Enron's collapse."[26]

In the Enron situation, Andersen correctly anticipated litigation - and government investigations - shortly before the issuance of a press release disclosing that Enron's shareholder equity would be reduced by $1.2 billion.[27] A week before issuing the release, Andersen, "which had an internal department of lawyers for routine legal matters, had retained an experienced New York law firm to handle future Enron-related litigation."[28] The Andersen indictment charged that these facts demonstrated Andersen was on notice of the obligation to preserve evidence in anticipation of litigation. The indictment alleged that

---

[22] *Id.* at *3-4.

[23] 18 U.S.C. § 1512(b)(2)

[24] *See* Indictment in *United States v. Arthur Andersen, LLP*, No. CRH-02-121 (S.D. Tex. Mar. 7, 2002). <http://news.findlaw.com/hdocs/docs/enron/usandersen030702ind.pdf>.

[25] *See, e.g.,* the Complaints in:

- *Severed Enron Employees Coalition v. Northern Trust Co*, No. H-02-0267 (S.D. Tex. Jan. 28, 2002) , <http://news.findlaw.com/hdocs/docs/enron/seecntrust012402cmp.pdf>;
- *Amalgamated Bank v. Lay, et al.*, consolidated into No. H-01-3624 (S.D. Tex. Dec. 4, 2001), <http://news.findlaw.com/hdocs/docs/enron/amlgmtd120401cmp.pdf>; and
- *Abrams v. Enron Corp., et al.*, No. H-01-3630 (S.D. Tex. Nov. 13, 2001) (Amended Complaint). <http://news.findlaw.com/hdocs/docs/enron/abrmsenron111301cmp.pdf>.

[26] Melody Petersen, "*Big Drug Company Says It May Face Obstruction Case*," N.Y. Times (May 31, 2003) (Schering-Plough announced "that it could soon be indicted in a federal investigation into its prescription drug marketing practices, and face charges that employees destroyed documents related to the case").

[27] Indictment, at 5 ¶ 8. <http://news.findlaw.com/hdocs/docs/enron/usandersen030702ind.pdf>.

[28] *Id.*

Andersen then embarked on an enormous spoliation effort.[29] In particular, it charged that, after weeks of shredding, "members of the Andersen team on the Enron audit were alerted finally that there could be 'no more shredding' because the firm had been 'officially served' [with a request] for documents."[30]

As part of the Enron fall-out, Congress included two information-tampering statutes in the vast Sarbanes-Oxley Act of 2002 ("Act").[31] The first one, § 802 of the Act, criminalizes the alteration of records related to federal investigations, bankruptcy proceedings and corporate audits.[32] The audit records component of Section 802 specifically references "electronic records."[33] The second one, §1102 of the Act, provides criminal penalties for "tampering with a record or otherwise impeding an official proceeding."[34]

Under state law, obstruction based on spoliation can also lead to criminal liability. For example, in California, one commits a misdemeanor if, "knowing that any book, paper, record, instrument in writing, or other matter or thing, is about to be produced in evidence upon any trial, inquiry, or investigation . . . willfully destroys, or conceals the same, with intent thereby to prevent it from being produced."[35]

3. When the Duty Arises

The duty to preserve evidence arises or expands upon the reasonable anticipation of litigation; receipt of pre-litigation correspondence; or service of the complaint, of the answer, or of discovery requests.

a. Pre-Litigation

Many courts have recognized a duty to preserve evidence that one knows, or reasonably should know, is relevant to pending, imminent, or reasonably foreseeable

---

[29] Indictment, at 5-6 10 (alleging that "an unparalleled initiative was undertaken to shred physical documentation and delete computer files. . . . The shredder at the ANDERSEN office at the Enron building was used virtually constantly. . . . A systematic effort was also undertaken and carried out to purge the computer hard-drives and E-mail system of Enron-related files."

[30] *Id.* at 6 ¶ 12.

[31] 116 Stat. 745, Pub. L. No. 107-204 (July 30, 2002), available at <http://www.loc.gov/law/guide/pl107204.pdf>. *See also* Michelle C. S. Lange, "*New act has major impact on electronic evidence*," (Nat'l L.J. Nov. 4, 2002), available at <http://www.nlj.com/toolbox/110402sarbanes.shtml>.

[32] 18 U.S.C. §§ 1519-1520.

[33] 18 U.S.C. § 1520(a)(2).

[34] 18 U.S.C. § 1512(c).

[35] California Penal Code § 135.

litigation.[36] In analyzing that duty, one California appellate court explained that "the character of . . . document destruction - whether illegal, unfair, immoral or not - is tied to, among other things, its timing."[37] That court described a "liability continuum" for destruction of evidence, beginning with the most egregious situation, namely documents about to be introduced into evidence at trial.[38] On the least culpable end of that continuum, "there is no liability for failing to preserve documents before a party has notice of their relevance to litigation likely to be commenced."[39] Whether a particular destruction situation ends up on that spectrum can depend on various factors, such as length of the pre-litigation period and the number of prior similar claims. [40]

b. After Service of Complaint

At a minimum, it is generally accepted that: "[s]ervice of a complaint puts the receiving party on notice that it is required to preserve evidence that may be relevant to the

---

[36] The preservation obligation arises upon "notice that . . . evidence is relevant to litigation - most commonly when suit has already been filed. . . but also on occasion in other circumstances, as for example when a party should have known that the evidence may be relevant to future litigation." *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998) (reversing summary judgment because jury could draw adverse inference from individual defendant's destruction of documents). *See also Mathias v. Jacobs*, 197 F.R.D. 29, 39 (S.D.N.Y. July 28, 2000) ("Obviously service of a discovery demand places a party on notice to preserve the materials explicitly requested, but the duty to preserve arises whenever a party has been served with a complaint or anticipates litigation." (citations omitted)), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/mathias.html>, *vacated in part on other grounds,* 167 F. Supp. 2d 606 (2001); *Shamis v. Ambassador Factors Corp.*, 34 F. Supp. 2d 879, 888-89 (S.D.N.Y. 1999) (" 'complaint itself may alert a party that certain information is relevant and likely to be sought in discovery' ") (citing *Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D. 68, 73 (S.D.N.Y. 1991) ("obligation to preserve evidence even arises prior to the filing of a complaint where a party is on notice that litigation is likely to be commenced")); *Winters v. Textron*, 187 F.R.D. 518, 520 (M.D. Pa. 1999) ("litigant is under a duty to preserve evidence which it knows or reasonably should know is relevant to the action. . . . [K]nowledge of a potential claim is deemed sufficient to impose a duty to preserve evidence.").

[37] *Willard v. Caterpillar, Inc.*, 40 Cal. App. 4th 892, 921, 48 Cal. Rptr. 2d 607 (1995) (noting the express prohibition of California Penal Code § 135).

[38] *Willard v. Caterpillar, Inc.,* 40 Cal. App. 4th 892, 921-22, 48 Cal. Rptr. 2d 607 (1995). California case law imposes sanctions for willful pre-litigation destruction of evidence that a putative defendant knew or should have known would have been relevant in a litigation. *Id*. at 921 (citing, e.g., *Wm. T. Thompson Co. v. General Nutrition Corp*., 593 F. Supp. 1443, 1455 (C.D. Cal. 1984) (sanctions appropriate where litigant has destroyed information it was on notice was "relevant to litigation, or potential litigation, or . . . reasonably calculated to lead to . . . discovery of admissible evidence), *overruled on other grounds*, *Cedars-Sinai Medical Center v. Superior Court*, 18 Cal. 4th 1, 11, 74 Cal. Rptr. 2d 248 (1998).

[39] 40 Cal. App. 4th at 922.

[40] *Willard* concluded that the facts before it fit within the last category, namely alleged spoliation too remotely relevant to justify the imposition of tort liability. *Id*. at 923. Given the evidence's disclosure of only one accident similar to Plaintiff's and in light of the lengthy passage of time, the trial court had erred in submitting to the jury Plaintiff's cause of action for intentional spoliation of evidence. *Id*. In *Cedars-Sinai Medical Ctr. v. Superior Court*, 18 Cal. 4th 1, 11, 74 Cal. Rptr. 2d 248 (1998) the Supreme Court of California subsequently rejected Willard's approval of the potential for tort liability for spoliation.

claims asserted."[41] That obligation arises before receipt of a production request.[42]

c. Once Discovery Process has Begun

The responsibility not to lose or destroy pertinent information intensifies once the discovery process is under way. For example, under the California Civil Procedure Code, sanctionable "[m]isuses of the discovery process include, but are not limited to:

- "Failing to respond or to submit to an authorized method of discovery."
- "Making an evasive response to discovery."
- "Disobeying a court order to provide discovery."[43]

4. What Must be Preserved

Once a complaint is filed, a litigant is obligated "to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request."[44] Generally speaking, a party should preserve those categories of evidence that it reasonably anticipates may later become

---

[41] *New York State NOW v. Cuomo*, 1998 U.S. Dist. LEXIS 10520, *5 (S.D.N.Y. July 14, 1998), *claim dismissed on other grounds sub nom. New York State NOW v. Pataki*, 261 F.3d 156 (2d Cir. 2001), *cert. denied*, 122 S. Ct. 1066 (2002). A party to a litigation has "a duty not to lose or destroy evidence relevant to the lawsuit." *Coca-Cola Bottling Co. v. Superior Court*, 233 Cal. App. 3d 1273, 1293 n.10, 286 Cal. Rptr. 855 (1991). *See also* Michael R. Overly, "*Overly on Electronic Evidence in California*" § 6.02 (West Group 1999) (citing *Coca-Cola Bottling* as authority for the existence of the duty to preserve evidence in litigation).

[42] *New York State NOW*, at *5 ("immaterial that the first document requests were not served until after the records were apparently destroyed; *Cedars-Sinai*, 18 Cal. 4th at 12 (destruction of evidence in anticipation of discovery request would be misuse of discovery).

[43] C.C.P. § 2023(a)(4), (6)-(7). *See also Cedars-Sinai Medical Ctr. v. Superior Court*, 18 Cal. 4th 1, 12, 74 Cal. Rptr. 2d 248 (1998) ("[d]estroying evidence in response to a discovery request . . . would surely be a misuse of discovery within the meaning of section 2023, as would such destruction in anticipation of a discovery request"); *R.S. Creative, Inc. v. Creative Cotton, Ltd*., 75 Cal. App. 4th 486, 89 Cal. Rptr. 2d 353 (1999) (dismissing complaint and imposing monetary sanctions under § 2023 for Plaintiffs' destruction of computer files during discovery).

Based on the availability of such sanctions under § 2023, the Supreme Court of California has declined to recognize a tort cause of action for intentional spoliation of evidence by a party. *Cedars-Sinai Medical Ctr. v. Superior Court*, 18 Cal. 4th 1, 11, 74 Cal. Rptr. 2d 248 (1998).

[44] *Wm. T. Thompson Co. v. General Nutrition Corp.*, 593 F. Supp. 1443, 1455 (C.D. Cal. 1984). *See also Danis v. USN Communics., Inc.,* 2000 WL 1694325, *32 (N.D. Ill. Oct. 23, 2000) (quoting Thompson), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/danis.html>; *China Ocean Shipping Co. v. Simone Metals Inc.*, 1999 U.S. Dist. LEXIS 16264, *12 (N.D. Ill. Sept. 30, 1999) ("duty to preserve evidence includes any relevant evidence over which the non-preserving entity had control and reasonably knew or could reasonably foresee was material to a potential legal action"); *Telectron, Inc. v. Overhead Door Corp.,* 116 F.R.D. 107, 127 (S.D. Fla. 1987); *Willard v. Caterpillar, Inc.,* 40 Cal. App. 4th 892, 921-22, 48 Cal. Rptr. 2d 607 (1995), overruled on other grounds, *Cedars-Sinai Medical Ctr. v. Superior Court*, 18 Cal. 4th 1, 11, 74 Cal. Rptr. 2d 248 (1998).

relevant.[45] For example, if the Defendant's business division and that division's product were mentioned repeatedly and prominently throughout the Plaintiff's complaint and requests for production, Defendant is obliged to preserve that division's sales correspondence and the like.[46]

Once the discovery process has begun, the preservation duty may prohibit not only file destruction, but also the ongoing use of electronic files. Earlier this year, a California appellate court affirmed the issuance of a temporary injunction to prevent defendants' ongoing use of certain electronic files they had taken from their former employer when they left to open their own company.[47] Only by "freez[ing]" defendants' electronically stored information in its then-current form could the court preclude the innocent or intentional alteration or destruction of evidence.[48] Because discovery sanctions can only punish abuse after it occurs, sanctions alone would have been an insufficient remedy at law.[49] In that preservation of the "status quo" was essential to protect Plaintiff's "right to the discovery,"[50] an injunction issued to prevent prospective file destruction.[51]

5. Attorney's and Client's Notification Obligations

Attorneys "have a duty to advise their clients of pending litigation and of the requirement to preserve potentially relevant evidence."[52] Because attorneys also have a duty to "establish a coherent and effective system to faithfully and effectively respond to discovery requests," they must also explain to their clients what types of information may constitute such potentially relevant evidence may encompass.[53] The most thorough communication would also inform a client of the range of potential negative consequences

---

[45] *Applied Telematics, Inc. v. Sprint Communics. Co.*, 1996 U.S. Dist. Lexis 14053, *6 (E.D. Pa. Sept. 17, 1996).

[46] *Telectron, Inc. v. Overhead Door Corp.*, 116 F.R.D. 107, 109-10 (S.D. Fla. 1987).

[47] Dodge, Warren & Peters Ins. Servs., Inc. v. Riley, 105 Cal. App. 4th 1414, 130 Cal. Rptr. 2d 385 (4 Dist. 2003).

[48] *Id.* at 1418.

[49] *Id.* at 1419-20.

[50] The court pointed out that, for preliminary injunction purposes in this context, the likelihood of success on the merits "concern[ed] whether there [was electronic] evidence" that Plaintiff will be able to discover – not the ultimate merits of Plaintiff's trade secrets and unfair business practices causes of action. *Id*. at 1418-20.

[51] *Id*. at 1419-20.

[52] *New York State NOW v. Cuomo*, 1998 U.S. Dist. LEXIS 10520, *5 (S.D.N.Y. July 14, 1998) (while failure to instruct defendant to retain documents in period between service of complaint and receipt of document requests potentially exposes counsel to sanctions, declining to impose sanctions where document destruction was neither in bad faith nor prejudicial to Plaintiff) (citing *Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D. 68, 73 (S.D.N.Y. 1991)(counsel has a "duty to advise his client of the type of information potentially relevant to the lawsuit and of the necessity of preventing its destruction").

[53] *Met*, 2003 U.S. Dist. LEXIS 1077 at *141, 153 (quoting *National Ass'n of Radiation Survivors v. Turnage*, 1987 U.S. Dist. LEXIS 3468, *556 (N.D. Cal. 1987)).

of destruction or deletion, including contempt of court, civil and criminal[54] penalties, default judgment,[55] or dismissal.[56]

In turn, corporate representatives are obliged to adequately identify the underlying subject matter and to provide guidance to employees as to the scope of retention.[57] A preservation order implicates a heightened obligation.[58] Notice of a preservation obligation should be disseminated in a manner most likely to reach the employees - for example, in hardcopy form as well as by e-mail.[59] In the event a relevant dispute ensues, it would be helpful to have proof of such notices, as well as a record of when and how they were communicated.

A court may impose severe sanctions, including entry of a default, for a party's failure to ensure that a preservation order is implemented and followed.[60] Some cautionary tales emanate from four federal district court decisions.

In one case, the Central District of California struck Defendant corporation's answer based on flagrant lack of compliance with a prior court order requiring the preservation of all purchase, sale, and inventory records maintained in the ordinary course of business.[61]

---

[54] *See, e.g.,* California Penal Code § 135 (possibility of misdemeanor conviction for destruction of relevant evidence).

[55] *Telectron*, 116 F.R.D. at 109-10 (imposing default judgment based on Defendant's corporate counsel's egregious conduct on day Complaint filed, namely instructing all employees to immediately destroy all sales correspondence over two years old generated by pertinent division of Defendant company).

[56] *Met*, 2003 U.S. Dist. LEXIS 1077 (S.D.N.Y. Jan. 28, 2003).

[57] *Turner*, 142 F.R.D. at 73 ("obligation to retain discoverable materials is an affirmative one; it requires that the agency or corporate officers having notice of discovery obligations communicate those obligations to employees in possession of discoverable materials").

[58] One federal district court imposed a monetary sanction of $1 million for a corporation's failure to adequately inform employees about the existence of a class action, a preservation order and the obligation to preserve evidence. *In re Prudential Ins. Co. of Am. Sales Practices Litig*., 169 F.R.D. 598, 600, 617 (D.N.J. 1997) (lawsuit relating to practices in sale of life insurance). In *Prudential*, senior management had not directed the dissemination of a preservation order to employees. 169 F.R.D. at 617. In addition, the e-mails sent by management did not mention the pending class action or the court's order; nor did those e-mails describe the potential penalties for contempt of court for destruction of evidence. *Id*. at 612.

[59] In *Prudential*, although various pertinent e-mail messages were sent, many employees did not, or could not, read e-mail and thus did not receive the communications. 169 F.R.D. at 613. Therefore, the use of e-mail communications was ineffective and failed to implement the court's preservation order. *Id.*

[60] *See, e.g., Illinois Tool Works, Inc. v. Metro Mark Prods.,* Ltd., 43 F. Supp. 2d 951 (N.D. Ill. 1999) (while noting that facts could have supported contempt finding, awarding reasonable attorney fees, expert fees and costs due to lack of compliance with order to preserve integrity of computers); *Wm. T. Thompson Co.*, 593 F. Supp. at 1456 (striking GNC's answer and dismissing GNC's complaint in another action). Cf. *Metropolitan Opera Ass'n v. Local 100 Hotel Empl. & Rest. Empl. Int'l Union*, 2003 U.S. Dist. LEXIS 1077 (S.D.N.Y. Jan. 28, 2003) ("Met") (granting Plaintiff's motion for judgment).; *Lang v. Hochman*, 77 Cal. App. 4th 1225, 92 Cal. Rptr. 2d 322 (2000) (affirming imposition of "terminating sanctions" and entry of $22 million default judgment against Defendants after they failed to comply with three discovery orders requiring production of electronic files and other documents).

[61] *Thompson*, 593 F. Supp. at 1447.

Neither Defendant's management nor its counsel had instructed employees to preserve such records. Indeed, the president issued a memorandum to all personnel advising that the court order did not require any change in the company's standard document retention/destruction policies or practices. The court found that the course of conduct before and after the preservation order had condoned practices that precipitated the bad faith destruction of critical evidence.[62]

In a New Jersey federal class action, after Defendant corporation's feeble notification, four of Defendant's field offices destroyed unauthorized sales materials as part of routine document destruction.[63] The court chastised management for failing to take an active role in formulating, implementing, or communicating a document retention policy.[64] Defendant's "haphazard and uncoordinated approach to document retention indisputably denied the party opponent potential evidence to establish facts in dispute."[65] Thus, the court drew the inference that the destroyed materials were relevant and, if available, would have led to successful proof of the claim.[66]

In the recent *Met* labor dispute case, Defendants and their counsel exhibited a complete lack of good faith regarding the discovery process.[67] Among the litany of bad acts warranting the supreme sanction of entry of judgment were:

> -- in response to [Plaintiff] Met counsel's continuing assertions of lack of an adequate document search and demonstrations of non-production, [Defendant] Union's counsel repeatedly represented to the Court that all . . . responsive document[s] . . . had been produced when . . . a thorough search had never been made and counsel had no basis for so representing;
>
> -- counsel knew the Union's files were in disarray and that it had no document retention policy but failed to cause a retention policy to be adopted to prevent destruction of responsive documents, both paper and electronic;

---

[62] *Id*. at 1447-48. Both before and after the entry of the preservation order, there had been a lack of preservation and a "failure to implement procedures to monitor or control document destruction." *Id.* at 1454. In addition, after the entry of the order, Defendant had: only preserved relatively useless bulk cash register tapes and store order strips; and erased computer tapes and disks that could have easily retained some of the stored information. *Id.*

[63] *In re Prudential Ins. Co. of Am. Sales Practices Litig.,* 169 F.R.D. 598, 615 (D.N.J. 1997).

[64] Upon entry of the document preservation order, "it became the obligation of senior management to initiate a comprehensive document preservation plan and to distribute it to all employees." *Prudential*, 169 F.R.D. at 615.

[65] *Id.*

[66] *Id.*

[67] "The Union and its counsel . . . failed to comply with their discovery obligations from the very outset of this action." *Met*, 2003 U.S. Dist. LEXIS 1077, * 164. For example, in lying to the court about a court-ordered deposition witness' vacation schedule, "counsel's conduct was not 'merely discourteous' but rather a breach of their responsibility to opposing counsel and the Court, inter alia, to engage in discovery in good faith, comply with court orders and, more fundamentally, to tell the truth." *Id*. at 164 (citing *Residential Funding*, 306 F.3d at 112).

-- counsel failed to explain to the non-lawyer in charge of document production . . . that a document included a draft or other non-identical copy and included documents in electronic form;

-- the non-lawyer the Union put in charge of document production failed to speak to all . . . who might have relevant documents, never followed up with the people [to whom] he did speak . . . and failed to contact all of the Union's internet service providers ("ISPs") to attempt to retrieve deleted e-mails as counsel represented to the Court that [the non-lawyer] would;

-- no lawyer ever doubled back to inquire of the Union employee in charge of document production whether he conducted a search and what steps he took to assure complete production; [and]

-- in the face of Met counsel's constant assertions that no adequate document search had been conducted and responsive documents had not been produced, Union counsel failed to inquire of several important witnesses about documents until the night before their depositions.[68]

The lengthy *Met* decision is a veritable guidebook on the notification aspect of the preservation, collection and production obligations.

Separate and apart from litigation ramifications for the corporation, corporate officers can be held personally responsible for the failure to preserve relevant evidence. For example, in one case the court imposed a $10,000 fine on the Chief Executive Officer (CEO) for breach of the duty to preserve.[69] In that situation, the CEO had delegated to the company's "inexperienced" general counsel the entire responsibility for implementing a document preservation plan.[70] In turn, the general counsel had neglected to develop specific retention criteria, to inform all employees in writing of the preservation duty, or to give written notice to employees of spoliation's impropriety and ramifications.

B. Scope of Preservation Duty - "Deleted" Files and Back-up Tapes

At the start of some cases, plaintiff serves a letter requesting that its opponent preserve all electronic information, including deleted files and file fragments, and cease modifying or deleting electronic information relating to pertinent topics.[71] At that early juncture, plaintiff "demand[s] preservation of 'all' electronic data, including every single

---

[68] *Id.* at *4-6.

[69] *Danis v. USN Communics., Inc.*, 2000 U.S. Dist. LEXIS 16900 (N.D. Ill. Oct. 23, 2000), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/danis.html>.

[70] *Id.*

[71] *See*, e.g., Richard A. Lazar, Esq., "*The Guide to Electronic Discovery*," 64-73 (2002) ("Fios Guide") ("appendix A: form spoliation letter to opposing counsel"), available upon free registration at <http://www.fiosinc.com/simplified/register.html>.

daily backup tape and file on a company system."[72]

1. "Deleted" Files

a. Introduction

"Deleted" does not necessarily mean gone forever.[73] Computer files that are deleted by the user are designated for deletion but remain on the system until they are overwritten randomly as the system needs the space. So, at any given time, a computer's hard drive may have "deleted" data that can be recovered. A sector-for-sector or copy of the hard drive will pick up any deleted files or file fragments that remain.[74] In contrast, a file-for-file copy of a hard drive does not pick up deleted files or file fragments, and some imaging programs overwrite some of the deleted files.[75] Given the ephemeral nature of electronic information, courts have been standing firm in enforcing the duty to preserve.[76]

b. Court-Ordered Hard Drive Searches

Does the obligation to search for and produce responsive computer data require a

---

[72] Electronic Evidence Discovery, Inc., "*A Balancing Act: Determining the Proper Level of Electronic Data Preservation*," Recent Developments, June 1998 (EEDI). *See also* Hon. James M. Rosenbaum, "*In Defense of the Delete Key*," 3 The Green Bag 393, 393 (Summer 2000) (observing that the "once-arcane fact [that nothing is truly deleted via the Delete key] has spawned a new legal industry: the mining of e-mails, computer files, and especially copies of hard drives to obtain deleted material"), available at <http://www.greenbag.org/rosenbaum_deletekey.pdf>. Note though, too overly broad a request can do more harm than good when one eventually appears before a judge on a discovery motion.

[73] *See Zubulake v. UBS Warburg LLC*, 2003 U.S. Dist. LEXIS 7939, *10 n.19 (S.D.N.Y. May 13, 2003) ("Warburg"), available at <http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/03-04265.PDF>; Hon. James M. Rosenbaum, "*In Defense of the Delete Key*," 3 The Green Bag 393 (Summer 2000).

[74] New Technologies, Inc.'s (NTI's) SafeBack software enables sector-by-sector copying via insertion into the target computer of a special bootable floppy disk that then pours the data out to a hard disk attached via the serial or parallel port. <http://www.forensics-intl.com/safeback.html>. Logicube's Forensic SF 5000 is a disk-copying device useable when one can remove the target hard drive from the computer. <http://www.logicubeforensics.com/>. *See also* Damian Tsoutsouris, "*Computer Forensic Legal Standards and Equipment*" (System Administration, Networking and Security Institute Dec. 6, 2001) (describing a prior iteration of the Forensic SF 5000 as "a hardware/software combination [that] has proven to be very effective"). <http://rr.sans.org/incident/legal_standards.php>.

[75] One should be careful to use the technically accurate terminology. The literature and cases refer to "imaging" a disk to preserve copies of deleted files and fragments. In fact, two of the more popular "imaging" programs each defragments a disk before copying it, thus overwriting some or all deleted files.

[76] *See* Christopher D. Wall & Michelle S. Lange, "*Electronic Discovery: Recent Developments*" (Wash. Lawyer Mar. 2003), noting that ("[s]imply booting a computer can possibly destroy valuable metadata (data about the data, such as *to, from, bcc,* and *date* fields in e-mail and the 'last accessed' or 'last modified' date in a document) that could be relevant in a lawsuit (citing *Antioch Co. v. Scrapbook Borders. Inc.*, 210 F.R.D. 645, 652-54 (D. Minn. 2002)).

search for "deleted" files?[77] Case law does not advise whether a diligent search for responsive information requires a search for deleted files. Yet, there have been cases in which a party successfully sought access to his opponent's computer to search for deleted files. If there is concrete evidence of destruction of electronic information, along with a basis for believing that such information may be discovered through a "deleted" file search of a hard drive, a court may grant such a request. However, the requesting party must: 1) establish that the burden and intrusion are justified by the need; and 2) show a reasonable basis for concluding that the search will turn up otherwise unavailable, responsive information.[78]

From 1999 to 2000, at least three federal court decisions granted requests for access to their opponents' computers.[79] It is not entirely clear whether there was concrete

---

[77] Parties' obligation to preserve electronic information does not necessarily extend to files deleted in the regular course of business. ABA Litigation Task Force Civil Discovery Standards 29(a)(iii) (Aug. 1999) (unless requesting party can demonstrate substantial need, ordinarily no duty "to try to restore electronic information . . . deleted or discarded in the regular course . . .but [maybe not] completely erased"). <http://www.abanet.org/litigation/taskforces/civil.doc>.

[78] *See Fennell v. First Steps Designs, Ltd.*, 83 F.3d 526 (1st Cir. 1996) (denying request to copy opponent's hard drive because no showing of particularized likelihood that information sought would be uncovered), also available at <http://laws.findlaw.com/1st/952294.html>; *Gates Rubber Co. v. Bando Chemical Indus., Ltd.*, 167 F.R.D. 90 (D. Colo. 1996) (rejecting argument that Defendant should have made a copy of employee's hard drive to preserve data designated for deletion; Plaintiff later obtained access to computer hard drive to find deleted data, but its computer technician bungled the search), available at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/gates.html>; *Strasser v. Yalamanchi*, 69 So.2d 1142 (Fla. 4th Dist. Ct. App. 1996) (denying access to opponent's hard drive to search for "purged" financial data in light of failure to prove likelihood of recovery), *review denied,* 805 So. 2d 810 (Fla. 2001).

[79] *See Playboy Enters., Inc. v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. 1999) (appointing neutral expert to copy Defendant's personal computer hard drive - due to evidence of Defendant's deletion of e-mails responsive to Plaintiff's document production request and likelihood of recovery), *aff'd in part and rev'd in part on other grounds*, 279 F.3d 796 (9th Cir. 2002) (without addressing any discovery issues, partially affirming summary judgment as to trademark claims); *Simon Property Group L.P. v. MySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. 2000) (appointing neutral expert to recover "deleted" files from computers, including home computers, used by Defendant's employees), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/process/simon.html>, *supp'd by*, 2000 U.S. Dist. 8953 (S.D. Ind. June 15, 2000); *Northwest Airlines, Inc. v. Local 2000 Int'l Brotherhood of Teamsters*, Civ. Action No. 00-08 (D. Minn. Feb. 2, 2000) (appointing neutral expert to examine and copy information and communications on home and office computer hard drives belonging to Defendants, who were union officers and rank-and-file union members).

Some of the described facts from *Northwest Airlines* are from Kenneth J. Withers, "*Computer-Based Discovery in Federal Civil Litigation*," 2000 Fed. Cts. L. Rev. 2 (Oct. 2000). <http://www.fclr.org/2000fedctslrev2.htm>. *See generally* "Case Study: Northwest Airlines" (Apr. 26, 2000) <http://cyber.law.harvard.edu/digitaldiscovery/digdisc_library_1.html>. A copy of the pertinent *Northwest Airlines* Order (containing the protocol), courtesy of Scott G. Knudson of Briggs and Moran, is available at <http://www.fenwick.com>. Note also that at least one commentator has questioned the neutrality of the *Northwest Airlines* expert. Sandra Rosenzweig, "*Rosie's Ramblings*" (Cal. Lawyer Dec. 2002) ("As Kenneth Shear, vice president of technology and law at Electronic Evidence Discovery . . . , tells it. . . Northwest and counsel for the union agreed on a court-approved discovery protocol that authorized . . . Northwest [to] cho[o]se its own accounting firm, Ernst & Young[,] . . . to copy the flight attendants' hard disks.").

evidence of data destruction in two of those cases.[80] In contrast, the third case[81] did involve actual data destruction. In any event, taken together, these three cases ostensibly ushered in a judicial tendency[82] to appoint a neutral expert to copy hard drives and to attempt to recover deleted data.

When a neutral computer forensics expert successfully flushes out a party's illicit tampering with e-mails, appropriate sanctions may very well follow.[83] In one such case, the neutral expert confirmed that Plaintiff had submitted an altered e-mail in opposition to a motion.[84] The court dismissed the complaint, ordering Plaintiff to reimburse Defendants for their portion of the expert's fee, and for attorney fees and costs reasonably connected to discovering the fraud perpetrated on the court. The court ruled that "[t]he ability to discover fraud . . . particularly sophisticated computer fraud, is greatly limited. Thus, the imposition of strong sanctions is one of the very few ways of deterring such activity in the future. This Court intends such a message here."[85]

In a subsequent decision not totally on point, a California court of appeal ruled that an employer could inspect the hard drive of a work-at-home computer it had provided to an employee.[86] The claims arose from an allegedly wrongful termination based on the employee's alleged intentional and repeated accessing of sexually explicit websites. The employee had consented in writing to the employer's policy of monitoring electronic communications conducted on office personal computers (PC's) as well as work-at-home PC's. Finding that, under Cal. Const. art. 1 § 1, "the employee had no reasonable expectation of privacy when he used the home computer for personal matters, the

[80] *Simon Property Group L.P. v. MySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. 2000), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/process/simon.html>, *supp'd by*, 2000 U.S. Dist. 8953 (S.D. Ind. June 15, 2000); *Northwest Airlines, Inc. v. Local 2000*, Civ. Action No. 00-08 (D. Minn. Feb. 2, 2000), is available at <http://www.fenwick.com>.

[81] *Playboy Enters., Inc. v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. 1999), *aff'd in part and rev'd in part on other grounds*, 279 F.3d 796 (9th Cir. 2002).

[82] *See Dodge, Warren & Peters Ins. Servs., Inc. v. Riley*, 105 Cal. App. 4th 1414, 1417, 130 Cal. Rptr. 385 (4 Dist. 2003) (affirming preliminary injunction freezing status quo and "requiring [Defendants] to allow a court-appointed expert to copy all [electronic storage media], to recover lost or deleted files and to perform automated searches of that evidence under guidelines agreed to by the parties or established by the court"); *Antioch Co. v. Scrapbook Borders. Inc.*, 210 F.R.D. 645, 652-54 (D. Minn. 2002) (in context of "resurrect[ing] data which ha[d] been deleted from Defendants' computer equipment," citing *Playboy and Simon* as authority for grant of Plaintiff's "Motion to Compel and Appoint a Neutral Expert in Computer Forensics").

[83] See *Munshani v. Signal Lake Venture Fund II*, 2001 Mass. Super. LEXIS 496 *3-4 (Oct. 9, 2001), also available at <http://www.signallake.com/litigation/ma_order_munhshani.pdf>, where Plaintiff submitted a copy of an e-mail as part of an opposition to a motion to dismiss on statute of frauds grounds. Defendant challenged the e-mail's authenticity, and Plaintiff proposed that the court "appoint its own neutral expert to collect all relevant evidence and ascertain the truth." *Id.* at *4. The court's expert determined, "in a 147-page detailed report," that the e-mail was "clearly not authentic." *Id.* at *5.

[84] *Munshani v. Signal Lake Venture Fund II*, 2001 Mass. Super. LEXIS 496, *5 (Oct. 9, 2001), also available at <http://www.signallake.com/litigation/ma_order_munhshani.pdf>.

[85] *Id.* at 7.

[86] *TBG Ins. Servs. Corp. v. Superior Court (Zieminski)*, 96 Cal. App. 4th 443, 445, 452-53, 117 Cal. Rptr. 2d 155 (2002).

appellate court directed the trial court to order the requested discovery."[87]

c. Sanctions for Heinous Deletions

Courts have looked with particular disfavor at parties whose spoliation consists of a deletion of files in defiance of a discovery order. In a trade secret misappropriation case, the court imposed sanctions on a former employee for such a transgression. The former employee had retained copies of a sensitive database and confidential e-mails containing customer information, and had taken them with him to his new job.[88] During discovery the court ordered him to turn over a copy of the database to his former employer, Lexis-Nexis, and not to retain any copies. Yet, he attempted to reconstruct the database on his new work laptop.[89] When the laptop was finally produced for inspection, Lexis-Nexis's forensic expert determined that the employee had deleted a number of important Lexis-Nexis documents that he had not earlier acknowledged possessing. The expert also found hundreds of additional Lexis-Nexis e-mails with sensitive company documents as attachments. The employee had not earlier acknowledged possessing those e-mails. Lexis-Nexis sought sanctions for spoliation. The court granted monetary sanctions against the employee for his discovery abuses and his clear violation of both parts of the discovery order. [90]

Even in the absence of a preservation order, a court may impose sanctions for deceitful conduct intended to destroy evidence relevant to a pending motion. In late 2001,

---

[87] *Id.* at 445, 452-53. Though a potential federal e-mail monitoring claim by an employee is beyond the scope of this paper, note that the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511(2)(h)(ii) allows "a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider . . . from fraudulent, unlawful or abusive use of such service."

[88] *Lexis-Nexis v. Beer*, 41 F. Supp. 2d 950 (D. Minn. 1999), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/lexis.html>. As he was leaving his employment with Lexis-Nexis, the employee copied onto a Zip disk sensitive company e-mails as well as a database containing customer information. He then took that information with him to his new job at Dow Jones Interactive Publishing, a direct Lexis-Nexis competitor. The employee transferred the e-mails and database to a new laptop he received from Dow Jones and then threw the Zip disk away.

[89] Upon learning of the steps he had taken, Plaintiff's counsel requested that Defendant's counsel take immediate possession of the laptop. Defendant's counsel did so, and then attempted to make a copy of the hard drive. During this attempt, counsel inadvertently overwrote the remnants of some previously deleted data. To avoid a similar fate, informed counsel should consider copying any disk that is thought to possibly contain relevant deleted files. Any effort to restore deleted information should use a duplicate of the disk to avoid complications that can result from botched restoration or retrieval activity.

[90] *Lexis-Nexis*, 41 F. Supp. 2d at 955. The court, however, declined to draw any adverse evidentiary inferences. *Id.* at 954-55. The court was not convinced that Lexis-Nexis could show that evidence pertinent to the litigation was actually destroyed. *Id.* at 954. In particular, it relied on the experts' reports indicating that ostensibly deleted documents were actually still present on the new laptop's hard drive. *Id.* Additionally, even if information had been deleted - for example, when Defendant's counsel overwrote inactive data while attempting to make a copy of the laptop hard drive - the court found that Lexis-Nexis had failed to demonstrate that the loss of this evidence would prejudice its case. *Id.* at 955 (relying on *Gates Rubber Co. v. Bando Chemical Indus.*, 167 F.R.D. 90, 104 (D. Colo. 1996), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/gates.html>).

the Northern District of California sanctioned a defendant for its egregious removal of website information in an attempt to avoid California personal jurisdiction.[91] In opposing a jurisdictional motion to dismiss, Plaintiff alleged that Defendant company had maintained a California office. Plaintiff submitted a printout of a page from Defendant's website that had displayed that office's contact information. The web page subsequently "disappeared" shortly after the filing of the motion. Defendant initially denied that the web page "ever existed on its web site or on any location authorized by Defendant."[92] Then, "[i]n a sudden resurgence of memory," Defendant recalled deleting the page "as part of 'routine maintenance,' but provided no details whatsoever about this alleged practice."[93] When faced with this obvious duplicity, the court sanctioned Defendant under Federal Rule 37(b)(2) as well as under its inherent judicial powers; the award included a monetary penalty, reasonable attorney fees, and costs.[94] Because Defendant eventually stipulated to jurisdiction, an order establishing personal jurisdiction pursuant to Rule 37(b)(2), while justified, was not necessary.[95]

2. Deleted Back-up Tapes

a. Background on Back-up Tapes

It is commonplace for companies to make daily or weekly computer system data back-ups, to have on hand in case of a catastrophic system crash. Typically, those back-up tapes are retained for a week, a month, or a similar period of time, and then are put back into rotation and recycled.[96] Each back-up takes a snapshot of the information on the computer system at the time of the back-up. When subsequent back-up tapes are made a day, a week, or a month later, previously created back-up tapes may be recycled or deleted from the back-up storage facility. Information on back-up tapes, once they are "restored," can be searched, extracted, or manipulated.

Although the cost of back-up tapes themselves is relatively small, the cost of restoring, reviewing, and extracting responsive information from back-up tapes can run into

---

[91] *Pennar Software Corp. v. Fortune 500 Systems, Ltd*., 2001 U.S. Dist. LEXIS 18432, *5 (N.D. Cal. Oct. 26, 2001).

[92] *Id.* at *5.

[93] *Id.* at *6.

[94] *Id.* at *14.

[95] *Id*. *Cf. Giardina v. Lockheed Martin Corp.*, 2003 WL 1338826 (E.D. La. Mar. 14, 2003) (in Title VII employment discrimination action, affirming magistrate's award of attorney fees under Fed. R. Civ. P. 37(a)(4)(A), due to Defendant's inadequate response to interrogatory seeking list of non-work-related websites visited by 16 computers in six-month period).

[96] *See, e.g., Linnen v. A. H. Robins Co.*, 10 Mass. L. Rptr. 189, 1999 Mass. Super. LEXIS 240 (June 16, 1999) (back-up tapes recycled every three months), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/linnen.html>.

tens of thousands of dollars.[97] Successive daily or weekly back-up tapes share much of the same data, the only difference being modifications or deletions. Thus, responding to a "blanket preservation order" by maintaining back-up tapes throughout the life of a lawsuit "would probably result in the accumulation of excessive duplicative and irrelevant data."[98]

A party has an obligation to preserve, search, and produce responsive information contained on computer media and in its computer system. Just how far must a party go to comply with this obligation? Must it cease the recycling of back-up tapes and set them aside indefinitely for possible use in the lawsuit? A back-up is by definition a copy of data already on the computer system. Thus, theoretically, at any given point in time, a party may fulfill its discovery obligations by: taking steps to preserve all pertinent data on its system; and searching for and collecting all potentially responsive information residing in that system at the given juncture. As long as the scope of discoverable information is delimited by a specific end date, coinciding with the date on which the preservation effort is made, then additional back-up tapes from later dates would not be important.[99] The ultimate answer, though, will depend upon a variety of factors, including:

- the judge;
- the underlying facts;
- the desires of the parties (e.g., has one party specifically requested back-up tapes?);
- the sufficiency of the responding party's efforts to search and preserve data on its computer system; and
- the scope of discoverable information - i.e., whether discoverable information is regularly being produced in the party's day-to-day business or whether the pertinent time period is relatively fixed in the past.

b. Failure to Cease Ordinary Recycling

Some courts have enforced preservation obligations regarding back-up tapes. For example, in one case, *Linnen v. A. H. Robins Co.*,[100] Plaintiff succeeded on a sanctions motion, based on a theory that Defendant's failure to preserve back-up tapes during the

---

[97] Corinne L. Giacobbe, Note, "*Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronically Stored Data*," 57 Wash. & Lee L. Rev. 257, 262 (2000) (hereafter "Giacobbe") (discovery of electronically-stored data can be extremely costly relative to hard copies, because companies tend to retain greater quantities of it and because it tends to linger in storage systems longer); Electronic Evidence Discovery, Inc., "*A Balancing Act: Determining the Proper Level of Electronic Data Preservation*" (Recent Developments, June 1998) (hereafter "EEDI").

[98] *Giacobbe*, 57 Wash. & Lee L. Rev. at 262.

[99] As a practical matter, this theoretical scenario will rarely, if ever, play out in this way because it would require the preserver to be sufficiently clairvoyant to identify an exact and accurate end date.

[100] 10 Mass. L. Rptr. 189, 1999 Mass. Super. LEXIS 240 (June 16, 1999), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/linnen.html>.

first four months of the lawsuit was tantamount to evidence destruction.[101] Plaintiff argued that pertinent e-mails and other information might have been deleted and therefore would only be available on back-up tapes. According to Plaintiff, the challenged four-month period was critical to the underlying product liability claim, in that it had immediately preceded Defendant's decision to remove from the market the relevant pharmaceutical product.

In light of an *ex parte* preservation order (albeit temporary) and the service of production requests, Defendant was obliged to preserve the back-up tapes.[102] Because Defendant did not fulfill that obligation, the court granted spoliation sanctions, including a jury instruction permitting the inference that Defendant had destroyed potentially relevant evidence out of a realization that the evidence was unfavorable.[103]

Similarly, another court imposed spoliation sanctions for a party's failure to preserve back-up tapes that were the only source of relevant information.[104] Defendant had not willfully destroyed salient telephone routing plans to prevent discovery of them. Rather, its computer system back-up files had been automatically deleted on a weekly basis, as part of normal operating procedures.[105] Once served with a document request, Defendant

---

[101] *Linnen*, 1999 Mass. Super. LEXIS 240, at *9 (upon receiving a preservation order or request for production encompasses computer media, Defendant must cease the recycling of back-up tapes and preserve those tapes for production. *Linnen* was a wrongful death action involving the weight-loss drug combination known as "fen/phen." The day the complaint was filed, Plaintiff obtained an ex parte preservation order. The court vacated the order a couple weeks later, but there theoretically remained "an understanding between the parties that the [items] would not be destroyed." Still another two weeks later, Plaintiff served document requests on one of the Defendants, a pharmaceutical company. Those requests broadly defined "documents" to include information stored in any computer medium. Yet Defendant continued to recycle its system back-up tapes under a three-month rotation schedule. It was not until three months after service of the discovery requests that Defendant ceased recycling the tapes and began setting them aside.

[102] In particular, the court ruled that:

> During the period of time when the *ex parte* order requiring [D]efendant to preserve all documents relating to this action was in effect, *the customary recycling of back-up tapes for the electronic mail system should have been suspended*. . . . The recycling, and resultant destruction, of those back-up tapes was in clear violation of the court's order. . . . [T]he request for production of documents defined the term "document" in a broad fashion, seeking "any record or compilation of information of any kind or description, however made . . . . or stored." Also requested were any documents in the form of computer memory or computer disk. . . . The language of the document request ma[de] it clear that [P]laintiffs sought the production of items such as the system back-up tapes and, after receiving this request, [D]efendant had an obligation to preserve any such documents or materials.

Id. at 29-30 (emphasis added).

[103] *Id.* at *37.

[104] *Applied Telematics, Inc. v. Sprint Communics. Co.*, 1996 U.S. Dist. Lexis 14053, *10-11, *14 (E.D. Pa. Sep. 17, 1996) (granting Plaintiff's motion for adverse inference of spoliation and for spoliation sanctions; also awarding reasonable attorney fees and costs).

[105] *Id.* at *11.

should have been aware that the routing plans were the subject of discovery. Thus, it was "at fault for not taking steps to prevent . . . routine deletion of . . . backup files."[106] The court rejected Defendant's putative excuse that Plaintiff had been previously informed of the routine deletion of back-up files but had not asked Defendant to save them.[107] Defendant had an independent, "affirmative" preservation duty. [108]

c. Restoring & Searching Back-up Tapes

While potentially costly, assuming an obligation to restore many back-up tapes in response to a discovery request "is one of the risks taken on by companies which have made the decision to avail themselves of the computer technology now available to the business world."[109] Courts are now unlikely to be swayed by a high tech company that balks at the prospect of back-up restoration. For example, in a product liability class action, *Linnen v. A. H. Robins Co.,*[110] the court did not look kindly on the lead Defendant's stonewalling. Robins had produced only a small number of e-mail messages, in hardcopy form, as of one year into the litigation. Plaintiff then requested the production of all e-mails, to or from 15 people, referencing three significant topics. After months of obfuscation and sporadic production, Defendant finally disclosed that it might have located thousands of old back-up tapes. It had apparently taken those tapes out of the recycling process in connection with another case, Case No. MDL 1203, which was a consolidated multi-district litigation action in which A. H. Robins Co. was also a party.

Plaintiffs narrowed the categories of responsive tapes by limiting the request to a shorter time frame, to a smaller number of persons, and to a narrower issue. However, Plaintiffs also broadened the request by seeking the restoration of all relevant back-up tapes, not just a sampling. The court agreed that the tapes "ha[d] the potential for containing relevant material and that Plaintiffs should have the opportunity to examine at least a portion . . . to determine if that is the case."[111]

Defendant argued that restoring and searching back-up tapes would be an unduly burdensome "multi-million dollar fishing expedition."[112] The court disagreed, noting that

---

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Linnen*, 1999 Mass. Super. LEXIS 240, at *18 ("[t]o permit a corporation such as [Defendant A.H. Robins, a large pharmaceutical company,] to reap the business benefits of such technology and simultaneously use that technology as a shield in litigation would lead to incongruous and unfair results"), <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/linnen.html>. *Cf. In re Brand Name Prescription Drugs Antitrust Litig.*, 1995 U.S. Dist. LEXIS 8281 (N.D. Ill. June 15, 1995) (if a party chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk), <http://cyber.law.harvard.edu/digitaldiscovery/library/cost/brandname.html>.

[110] *Linnen*, 1999 Mass. Super LEXIS 240.

[111] *Id.* at *16.

[112] *Id.* at *17.

Plaintiffs had tailored the request to seek specific responsive e-mails.[113] The court declined to order the restoration and search of all the requested back-up tapes. It held that the parties should await the MDL 1203 restoration and sampling search results, which Defendant would produce to Plaintiffs. Then, Plaintiffs could revisit their request for production.[114]

---

[113] The court rejected Defendant's argument that the number of previously produced documents (including e-mails) somehow affected Plaintiff's right to additional discovery. *Id.* at *17 n.6. *See also Cobell v. Norton*, 2002 U.S. Dist. LEXIS 5291, at *4-5 (D.D.C. Mar. 29, 2002) (in light of court's prior rejection of same arguments, sanctioning Defendant Department of Interior for seeking a " 'protective order clarifying that it may produce e-mail in response to discovery requests by producing from [sic] paper records of e-mail messages rather than from backup tapes and may overwrite backup tapes in accordance with Departmental directives.' " *Cf. Cobell v. Norton*, 2002 U.S. Dist. LEXIS 5292 (D.D.C. Mar. 29, 2002). The Government's many discovery abuses in Cobell ultimately contributed to the court's issuance of multiple civil contempt orders. *See Cobell v. Norton*, 2002 U.S. Dist. LEXIS 17353 (D.D.C. Sep. 17, 2002) (267 page opinion finding Interior Department's Secretary as well as its Assistant Secretary of Interior for Indian Affairs in civil contempt for failing to comply with prior order to initiate historical accounting project on Individual Indian Money trust funds).

[114] In one of the fen-phen litigations, a Plaintiff's computer forensics experts uncovered a "smoking gun" e-mail message, which was ultimately leaked to the press. Depending on which article one reads, the message is attributed to a different individual – *e.g.,* an accountant at A.H. Robins' successor American Home Products (AHP) or an administrator at AHP's subsidiary Wyeth-Aherst Laboratories. The message is universally claimed to have read: "Do I have to look forward to my waning years writing checks to fat people with a silly lung problem?" Kristin M. Nimsger, "*Same Game, New Rules; E-discovery adds complexity to protecting clients and disadvantaging opponents*" (Legal Times June 18, 2002), available at<http://www.law.com/special/supplement/e_discovery/same_game.html>; J. Robert Keena, "*E-Discovery: Unearthing Documents Byte by Byte*" (Bench & Bar of Minn. Mar. 2, 2002) ("Keena"), <http://www2.mnbar.org/benchandbar/2002/mar02/ediscovery.htm>.

The take-away, according to Keena:

> Once discovery begins, the chase is on for smoking gun e-mails, memos admitting liability, deleted design documents, and other documents never intended to see the light of day. Simply adding a request for e-mails and electronic documents to a standard discovery request will not likely inspire an opponent to conduct such a forensic search. Specific requests, clearly aimed at electronic evidence, are needed instead. It has been proven time and time again that e-mails are fertile ground for unearthing damaging documents. Individuals believe them to be private communication.

Cf. Ann Carns, "*Those Bawdy E-Mails Were Good For a Laugh – Until the Ax Fell,*" 2000 WL-WSJ 3016760 (WSJ Feb. 4, 2000), <http://www.loper.org/~george/trends/2000/Feb/97.html>:

> [I]n harassment suits[,] one or two explicit e-mail messages typically aren't enough by themselves to prove that a workplace environment was hostile. But such e-mail can bolster other damaging evidence. At a subsidiary of Chevron Corp., e-mail containing such jokes as '25 reasons beer is better than women' were used along with other evidence in a sexual-harassment claim that was settled in 1995 for $2.2 million.

In a more recent decision, *McPeek v. Ashcroft*[115], the District of Columbia federal district court noted that "[t]here is certainly no controlling authority for the proposition that restoring all backup tapes is necessary in every case." Mindful of the costs involved and the lack of precedent, the court "decided to take small steps and perform, as it were, a test run" to determine if the costs associated with a backup search were justified by relevant results.[116]

In *McPeek*, Plaintiff had sought to force the Department of Justice (DOJ) to search for backup copies of deleted files that might relate to retaliation that Plaintiff claimed to have suffered because he complained about sexual harassment. The court recognized the high cost that the DOJ would incur to produce backups.[117] Part of the cost at hand stemmed from the indiscriminate way back-up tapes collect information and the nature of the DOJ computer system – designed "not for the purpose of creating a [copy] of each user's hard drive [but] to prevent disaster."[118] As a result, the court only ordered the DOJ to perform a backup restoration and search of the e-mails to and from Plaintiff's supervisor for a one-year period.[119]

Even more recently, a Second Circuit jury verdict reversal reinforced the judicial trend to scrutinize companies' contentions that they cannot recover data stored on back-up tapes. In *Residential Funding Corp. v. DeGeorge Financial Corp.*,[120] the appellate court found that the trial court had not adequately dissected Plaintiff's months of protestations concerning purported technical difficulties in recovering e-mails from the critical time period at issue. Those contentions, which had continued past the start of trial, were rendered quite suspicious by Defendant's consultant's ability, to recover 950,000 e-mails from the

---

[115] *McPeek v. Ashcroft*, 202 F.R.D. 31, 34 (D.D.C. 2001). ("*McPeek I*"). Almost a year and a half later, once the search was complete, the parties returned to court. *See McPeek v. Ashcroft*, 212 F.R. D. 33, 34 (D.D.C. 2003). The parties vehemently disagreed as to their characterizations of the search results. Plaintiff contended that the search had "produced useful, relevant information that justif[ied] a second [easy, inexpensive] search of backup tapes for certain periods. . . . . Defendant . . . insist[ed] that the first search only produced [cumulative] documents . . . and a second search would be expensive and time consuming." After "assess[ing] . . . the likelihood that [the back-up tapes would contain . . . word processing documents and e-mails . . .that w[ould] produce information that is relevant to the lawsuit," the judge denied the request for additional searches as to three of the four individuals at issue. *McPeek II*, 212 F.R.D. at 34. *But compare Amsted Indus. "ERISA" Litig.,* 2202 WL 31844956, *2 (N.D. Ill. Dec. 18, 2002) (in breach of fiduciary duty action as to Employee Stock Option Plan, ordering additional, broader searches of previously searched e-mail back-up tapes).

[116] *McPeek I*, 202 F.R.D. at 34.

[117] *Id.* at 32 ("merely restoring the e-mail from a single backup tape would take eight hours at a cost of no less than $93 per hour").

[118] *Id.* at 33 ("[b]ackup tapes are by their nature indiscriminate[; t]hey capture all information at a given time and from a given server but do not catalogue it by subject matter").

[119] *Id.* at 34-35 (choosing that timeframe "because a letter from [P]laintiff's counsel to DOJ, complaining of retaliation and threatening to file an administrative claim," was dated one day before the start of the year to be restored; and the court was "hoping that the restoration w[ould] yield both the e-mails [Plaintiff's supervisor] sent and those he received").

[120] 2002 U.S. App. LEXIS 20422, *13.

pertinent time period in four days.[121]

On the other end of the spectrum, a party that will not narrow an overly broad request should expect judicial disdain. As the Eleventh Circuit noted this past winter:[122]

> [Plaintiff] sought discovery of a "computer diskette or tape copy of all word processing files created, modified and/or accessed by, or on behalf" of five [of Defendant's] employees over a two and one-half year period. [Plaintiff] made no attempt to narrow his request to something more meaningful and relevant during the discovery period despite an appropriate objection from [Defendant]. . . .
>
> On appeal, [Plaintiff] has not tried to identify particular items within the expansive request nor has he provided a theory of relevance that might narrow the scope of his request.[123]

The appellate court therefore affirmed the denial of a motion to compel premised on the overbroad request.

The most recent restoration decision occurred in a Southern District of New York case discussed in more detail in Section II(D)(4) below. There, in the context of assessing the likelihood of discovering relevant evidence on inaccessible media such as back-up tapes, the court adopted a "small sample . . . fact-intensive" approach:[124]

> Requiring the responding party to restore and produce responsive documents from a small sample of backup tapes will inform the cost-shifting analysis. . . . When based on an actual sample, the marginal utility test will not be an exercise in speculation -- there will be tangible evidence of what the backup tapes may have to offer. There will also be tangible evidence of the time and cost required to restore the backup tapes, which in turn will inform the second group of cost-shifting factors. Thus, by requiring a sample restoration of backup tapes, the entire cost-shifting analysis can be grounded in fact rather than guesswork.

Consequently, the *Warburg* court directed the parties to return to court for the cost-shifting analysis only after Defendant had "produce[d], at its expense, responsive e-mails from any five [of the 94 pertinent] backups tapes selected by [Plaintiff and had] then prepared an affidavit detailing the results of its search, as well as the time and money spent."[125]

---

[121] *Id.* *34-37.

[122] *Wright v. AmSouth Bancorp.*, 2003 WL 245588 (11th Cir. Feb. 5, 2003) (affirming denial of discovery in ADEA illegal termination case), available at <http://www.law.emory.edu/11circuit/feb2003/02-10006.opn.html>.

[123] *Id.* at *6.

[124] *Warburg*, 2003 U.S. Dist. LEXIS 7939, *46-49 (S.D.N.Y. May 13, 2003) (citing *McPeek I*, 202 F.R.D. at 34-35), also available at <http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/03-04265.PDF>.

[125] *Id.* at *50.

C. Inspection of Opponent's Computer System

A party might request to inspect its opponent's computer system to search for electronic information. Sometimes parties agree that a computer system will be made available for expert inspection and/or copying.[126] If, however, the parties do not agree that computers or a computer system should be produced for inspection or copying, the requesting party must be able to explain the need for that discovery. Courts typically require evidence that the search will locate responsive information; any inconvenience will be justified; and the chances for harm will be minimized.[127]

This requirement was illustrated in *Fennell v. First Step Designs, Ltd.*,[128] a discrimination case, in which a discharged employee sought creation-date evidence for a memorandum regarding some layoffs, including her own. Defendant produced a copy of the memo on computer disk. When Plaintiff could not determine the creation date, she sought access to Defendant's computer hard drive. The parties' competing computer experts disagreed as to whether dates of creation and last modification could be determined from the hard drive. The district court held a hearing and "directed the parties to submit a 'protocol' establishing procedures by which [Plaintiff] would have access to relevant materials."[129] Defendant objected to Plaintiff's proposed protocol, which entailed a technician copying the entire hard drive, analyzing the copy off site, and later erasing the copy.[130] Defendant submitted its own detailed protocol, which the court described as "extremely cumbersome and expensive."[131]

After reviewing the competing protocols and "apparently recognizing that the parties were unlikely to reach consensus," the district court reversed its earlier decision to permit additional discovery.[132] It concluded that the hard drive copying presented a low likelihood

---

[126] *See, e.g., R.S. Creative, Inc. v. Creative Cotton, Ltd.*, 75 Cal. App. 4th 486, 490, 89 Cal. Rptr. 2d 353, 356 (1999) (imposing terminating sanctions based on Plaintiff's deletion of files, in violation of stipulation that "computers and diskettes would not be operated or touched . . . until [D]efendants' computer expert could examine them").

[127] *See, e.g., Fennell v. First Step Designs, Ltd.*, 83 F.3d 526 (1st Cir. 1996), also available at <http://laws.findlaw.com/1st/952294.html>; *Simon Property Group L.P. v. MySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. 2000), *supp'd by*, 2000 U.S. Dist. 8953 (S.D. Ind. June 15, 2000); *Northwest Airlines, Inc. v. Local 2000 Int'l Brotherhood of Teamsters*, Civ. Action No. 00-08 (D. Minn. Feb. 2, 2000); *Playboy Enters., Inc. v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. 1999), aff'd in part & rev'd in part on other grounds, 279 F.3d 796 (9th Cir. 2002).

[128] 83 F.3d 526 (1st Cir. 1996).

[129] *Fennell*, 83 F.3d at 530-32 (instructing that the procedure should minimize the intrusion into, and interference with, Defendant's operations and should assure confidentiality), also available at <http://laws.findlaw.com/1st/952294.html>.

[130] *Id.* at 532 (Defendant claimed Plaintiff's protocol: failed to describe the methodology by which the technician would determine the creation and modification dates; presented risks from accidental data loss, incompatible hardware and system downtime; did not adequately address attorney-client privilege and work product concerns as to documents on the hard drive; and allowed unsupervised possession of the copy).

[131] *Id.*

[132] *Id.*

of success, along with substantial risks and costs.[133] The First Circuit affirmed, noting that the lack of detail in Plaintiff's protocol "cast even more doubt on the soundness of the technical basis for the discovery venture."[134]

Similarly, a state court of appeal reversed an order that had given Plaintiff unlimited access to Defendant's computer system in *Strasser v. Yalamanchi*.[135] In Strasser, Plaintiff/doctor sought to inspect the computer system of Defendant, his ex-colleague. Plaintiff desired to locate and recover previously purged financial data. Defendant objected, claiming that the search would "allow carte blanche access, unlimited in scope, nature or purpose."[136] Ultimately, the trial court ordered the requested discovery. On appeal, though, the court agreed with Defendant that unfettered access was inapt, especially given the lack of any solid evidence of data recoverability.[137] Moreover, even had there been recoverability evidence, a tailored search would have been justified only if no other less intrusive means existed.[138]

In each of the decisions highlighted in Section II(B)(1)(b) above, a court has appointed a neutral computer expert to copy Defendant's to-be-searched computer hard drive(s) to try to recover deleted files.[139] Each court required that the requesting party, Plaintiff, would pay the expert's resultant fees and costs.[140] Additionally, in each case, to address concerns about possible attorney-client privilege waiver, each expert had to agree to the terms of the respective protective order, and the data recovered by the expert was to be turned over to defense counsel for pre-production review for privilege and

---

[133] *Id.*

[134] *Id.* at 533.

[135] *Strasser v. Yalamanchi*, 669 So.2d 1142 (Fla. 4th Dist. Ct. App. 1996), *review denied,* 805 So. 2d 810 (Fla. 2001).

[136] *Id.* at 1144. Defendant also claimed it would: constitute a wholesale intrusion into all proprietary business files and statutorily-protected patient information; and expose the system to harm through inadvertent deletion of files or the introduction of a virus.

[137] *Id.*

[138] *Id.* In that event, the trial court would have to "define parameters of time and scope, and . . . place sufficient access restrictions to prevent compromising patient confidentiality and to prevent harm to [D]efendant's computer and databases."

[139] *Simon Property Group L.P. v. MySimon, Inc.*, 194 F.R.D. 639, 641 (S.D. Ind. 2000) supp'd by, 2000 U.S. Dist. 8953 (S.D. Ind. June 15, 2000); *Northwest Airlines, Inc. v. Local 2000 Int'l Brotherhood of Teamsters*, Civ. Action No. 00-08 (D. Minn. Feb. 2, 2000); *Playboy Enters., Inc. v. Welles*, 60 F. Supp. 2d 1050,1055 (S.D. Cal. 1999), aff'd in part and rev'd in part on other grounds, 279 F.3d 796 (9th Cir. 2002). For URL's for *Simon* and *Northwest, see* note 100 *supra*. *See also Antioch Co. v. Scrapbook Borders. Inc.*, 210 F.R.D. 645, 652-54 (D. Minn. 2002).

[140] *Simon*, 194 F.R.D. at 641; *Northwest*, No. 00-08, Protocol, at 3, ¶ 5; *Welles*, 60 F. Supp. 2d at 1054-55 & n.6.

responsiveness.[141]

D. The Logistics of Producing Electronic Information

1. Production of Compilations of Electronic Information

Although the duty to preserve and produce back-up tapes and deleted files is a relatively novel issue, the general obligation to produce electronic information is well-established. The production of information in hardcopy form does not preclude the requesting party from receiving that same information in computerized form.[142] A court also may require a party to compile electronic data into a particular format or structure requested by the opposing party.[143] If a request is burdensome, a court may require the requesting party to not only show the need for the information but also agree to pay the costs of production.[144] If the respective merits of the justification-versus-burden analysis are uncertain, the court may order the parties to the negotiating table.[145]

2. Compelling Creation of Electronic Information

In a peer-to-peer (P2P) copyright infringement suit, the Central District of California ruled that a technology provider cannot be required to collect and produce data regarding its customers' use of its product.[146] The suit was brought by television executives and movie studios regarding the Replay TV 4000, a personal video recorder (PVR) that enables users to, among other things, store television programs for later viewing and to skip commercials when replaying a show.

---

[141] *Simon*, 194 F.R.D. at 641; *Northwest*, No. 00-08, Protocol, at 3, ¶ 9; *Welles*, 60 F. Supp. 2d at 1055. An example of a protective order encompassing privilege issues accompanies the decision in *United States v. Sungard Data Systems*, 173 F. Supp. 2d. 24-30 (D.D.C. 2001) (extending confidential information access to two in-house attorneys for each Defendant, contingent on their compliance with protective order). *See also Antioch Co. v. Scrapbook Borders. Inc.*, 210 F.R.D. 645, 652-54 (D. Minn. 2002).

[142] *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995-2 Trade Cases (CCH) ¶ 71,218, 1995 U.S. Dist. LEXIS 16355, 1995 WL 649934, *2 (S.D.N.Y. Nov. 3, 1995), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/process/antimonopoly.html>.

[143] *Anti-Monopoly*, 1995 U.S. Dist. LEXIS 16355, at *1 ("producing party can be required to design a computer program to extract [aggregate reports] from its computerized business records, subject to the Court's discretion as to the allocation of [design] costs"). *See also National Union Elec. Corp. v. Matsushita Elec. Indus. Co.*, 494 F. Supp. 1257, 1258-59 (E.D. Pa. 1980) (in antitrust case, requiring Plaintiff to rerun program causing its computer to assemble and print sales data onto computer-readable media such as magnetic tape; Defendants volunteered to pay cost). But see Replay decision discussed in Section II(D)(2).

[144] *Anti-Monopoly* , 1995 U.S. Dist. LEXIS 16355, at *3.

[145] *See Anti Monopoly*, where Plaintiff sought production in electronic form of every invoice and credit memo generated by Defendant over a four year period. Determining that it had insufficient information to weigh the purported justification against the alleged burden, the court asked the parties to negotiate.

[146] *Paramount Corp., et al. v. Replay TV, Inc. and SONICblue, Inc.*, No. CV 01-9358-FMC (Ex), Order (C.D. Cal. May 30, 2002), available at <http://www.fenwick.com> For many pleadings and decisions in the Replay TV case, see the Replay TV segment of the Privacy Law Resources page maintained by the authors' firm, Fenwick & West LLP ("F&W") at <http://www.fenwick.com>. Defendant SONICblue, Inc. was represented in that litigation by F&W.

Plaintiffs had sought discovery of documents and information regarding Defendants' customers, including identification of the television shows that the customers had recorded. In support of their request, Plaintiffs contended that "there [wa]s nothing unusual about directing a party to create software to 'retrieve information stored in computers.'"[147] They argued that there is "a duty to extract relevant information to respond to an interrogatory."[148]

Initially, the Magistrate Judge ordered the requested discovery.[149] Defendants obtained a stay of the Magistrate's order upon filing a motion for District Judge review of the order compelling discovery.[150] In their motion for review, Defendants emphasized that the requested items were never in their possession because they have opted not to monitor customer usage.[151] They contended that reinstatement of the discovery order would improperly force them to:

> design and develop new software to operate the ReplayTV 4000. Plaintiffs have insisted that Defendants install that reformulated product into units within consumers' homes to silently monitor private television viewing behavior and generate new electronic data about such uses. The product would then have to transmit that new electronic data from the consumers' home units to Defendants' servers, to be stored indefinitely, and made available to Plaintiffs in th[e] litigation.[152]

Defendants contended that the Magistrate's order would "not merely direct [them] to write ancillary software to extract or process in a new way the data it already possesses" but also to create software that would not process any information already contained in

---

[147] *See Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 362 (1978). Supplemental Brief in Support of Motion to Compel, at 4, PDF page 5 (Apr. 11, 2002), available at <http://www.fenwick.com>.

[148] Supplemental Brief in Support of Motion to Compel, at 4, PDF page 5 (Apr. 11, 2002). <http://www.fenwick.com>. In support of this proposition, Plaintiffs cited:

> *Jones v. Syntex Labs., Inc.,* No. 99C3113, 2001 WL 1338987, at *3 (N.D. Ill. 2001) ('duty to fully answer [interrogatory] implies a duty to make reasonable efforts to obtain information within the knowledge and possession of others.'); *PHE, Inc. v. Dep't of Justice*, 139 F.R.D. 249, 257 (D.D.C. 1991) (requiring party responding to interrogatories to retrieve computerized information about their distribution operations '[a]lthough no program may presently exist to obtain the information requested'); *Henderson v. Nat'l R.R. Passenger Corp.,* 113 F.R.D. 502, 507 (N.D. Ill. 1986) (ordering responding party to provide information and documents necessary to enable plaintiff to develop "sufficient statistical base" as evidence of claim).

Id. at 4.

[149] Minute Order, at 1 (Apr. 26, 2002), available at <http://www.fenwick.com>.

[150] All of Defendants' papers in support of their Ex Parte Application for Stay and their Motion for Review are linked off of <http://www.fenwick.com>.

[151] Defendants' Brief in Support of Motion for Review ("Review Brief"), at 25 (May 10, 2002), available at <http://www.fenwick.com>.

[152] *Id.* at 2.

[their] servers."[153] Defendants asked the court to distinguish prior compilation production cases[154] as having entailed either retrieval or software design to enable the extraction of already extant electronic business records.[155] They posited that, in contrast, a party cannot be "required 'to prepare, or cause to be prepared,' new documents solely for their production."[156]

The Replay TV defendants also argued that "[w]hile Rule 34 may require compilations from existing databases, no authority supports the proposition that Rule 34 can require creation of new data that never existed - much less the reformulation of a consumer product to create such data."[157] The district court judge accepted Defendants' interpretation of Rule 34, ruling that "the information sought by [P][laintiffs is not now and has never been in existence. The [portion of the Magistrate's] Order requiring its production is therefore contrary to law."[158] That determination may have a great impact on future discovery disputes in which one party seeks to compel another to compile, manipulate and/or generate data.

3. Facilitating Opponent's Access of Electronic Information

A court may require the producing party to make it easier for the requesting party to access electronic information as an alternative to ordering massive hardcopy production. For example, in an employment discrimination case, the Seventh Circuit upheld the trial court's decision to deny Plaintiff's motion to compel production of what would have amounted to 210,000 hardcopy pages of e-mails.[159] Defendant had initially produced the e-mails on four-inch tapes, an inaccessible format for Plaintiff/employee's counsel, who had neither the software nor the equipment to read them. To accommodate the employee, the district court required the employer to: download the data from the tapes to conventional computer disks or a computer hard drive; loan the employee a copy of the

---

[153] *Id.*

[154] *PHE, Inc. v. Dep't of Justice*, 139 F.R.D. 249, 257 (D.D.C. 1991); *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 U.S. Dist. LEXIS 16355 (S.D.N.Y. Mar. 28, 2000), available at <http://cyber.law.harvard.edu/digitaldiscovery/library/process/antimonopoly.html>.

[155] Review Brief (May 10, 2002) at 7, n.7, PDF page 14, n. 7, available at <http://www.fenwick.com>, arguing:

> [A] party cannot be required to create, either in paper or electronic form, documents or data that do not currently exist within its possession. *Hill v. McHenry*, Civil Action No. 99-2026-CM, 2002 U.S. Dist. LEXIS 8033 (D. Kan. April 30, 2002) (court "cannot compel the production of documents that do not exist"). Rule 34 "only requires a party to produce documents that are already in existence." *Alexander v. FBI*, 194 F.R.D. 305, 310 (D.D.C. 2000).

[156] Review Brief (May 10, 2002) at 8, PDF p. 15.

[157] Review Brief (May 10, 2002) at 8, PDF p. 15.

[158] Order (May 30, 2002), at 5, PDF p. 8, available at <http://www.fenwick.com> (citing *National Union Elec. Corp. v. Matsushita Elec. Indus. Co.*, 494 F. Supp. 1257, 1258-59 (E.D. Pa. 1980)).

[159] *Sattar v. Motorola, Inc.*, 138 F.3d 1164 (7th Cir. 1998), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/process/sattar.html>.

necessary software; or offer him on-site access to its own system.[160] Only if those options had ultimately failed (they did not) would the court have ordered the parties to split the cost of copying the e-mails in hardcopy form.[161]

In a 2002 Southern District of New York decision, *Goord v. Jones*, practical considerations seemed to hamstring a judge who might otherwise have required Defendant to produce "data in electronic, manipulable form [to] facilitate expert analysis."[162] *Goord* entails a class action brought by inmates to challenge the "double-celling" practice of the New York State Department of Corrective Services ("DOCS"). Nearly six years into the litigation, the inmates sought production of electronic records and databases maintained by state correctional authorities. Judge Lynch explained that:

> [T]he expert affidavits supplied by defendants, and uncontradicted by any evidence offered by plaintiffs, persuasively establish that . . . [b]ecause the databases were designed for the operational purposes of prison administrators, the data desired by plaintiffs, while perhaps present in the databases, are not readily available for the statistical manipulations proposed by plaintiffs. . . . Thus, the databases in question are not simply collections of lists or numbers that can be easily extracted and correlated with other numbers; rather, each of the requested databases has 'been constructed to support the interactions of hundreds of concurrent users rather than to support the analytical activities of a few.' . . .
>
> Thus, providing plaintiffs with any meaningful access to aspects of this system is not a matter of duplicating discs and handing over copies. The data that would presumably be useful to plaintiffs in analyzing patterns of disease and violence or correlating such patterns with double-celled inmates are not simply numbers maintained in a simple set of files that can be downloaded into some (unspecified) statistical analytic program and then crunched in some (unspecified) way to produce meaningful results. DOCS personnel would need to prepare extensive documentation of the structure of the programs and databases to enable any experts retained by plaintiffs to understand the layout of the data, the meaning of codes, and the sources from which those codes can be derived.[163]

Four practical considerations doomed Plaintiff's "plausible claim" that "manipulable

---

[160] *Id.* at 1171. *Cf. GTFM, Inc. v. Wal-Mart Stores*, 2000 U.S. Dist. LEXIS 3804, 2000 WL 335558, *1 (S.D.N.Y. Mar. 30, 2000) (ordering Defendant to make available person most familiar with its computer records to provide reasonable assistance while Plaintiffs' data retrieval expert would be given computer access).

[161] *Sattar v. Motorola, Inc.*, 138 F.3d 1164, 1171 (7th Cir. 1998)

[162] *Jones v. Goord*, 2002 U.S. Dist. LEXIS 8707, *39 (S.D.N.Y. May 16, 2002).

[163] *Id.* at *28-29, 31.

data" was needed.[164] First, even though he acknowledged the financial constraints of pro bono counsel, the judge was troubled by Plaintiffs' lack of an expert; this deficiency had rendered Plaintiffs' discovery plan quite general.[165] Second, much of what the inmates hoped to discover was contained in more than 700,000 pages of hardcopy records already produced in paper form, at considerable state expense.[166] Third, the factual context entailed the same type of "significant security[/confidentiality] concerns" typically found in trade secrets cases "in a business context."[167]

Lastly, Plaintiffs' request had been made very late in a case that had been pending for more than six years and after numerous extensions of the discovery cutoff date.[168] Therefore, the court declined to "impose additional burden, expense and risk of harm on the parties, and especially on [D]efendants, at this belated hour, after the expenditure of so much effort and expense, and on the undocumented hope of obtaining such speculative benefits."[169]

In contrast, in another civil case against the government, a state's highest court went quite far in finding the discoverability of electronic reports and databases.[170] The discovery dispute in *Guillen v. Pierce County* arose when, to develop a wrongful death claim, a widower filed a separate lawsuit seeking disclosure of historical traffic accident reports. Even though relevant federal and state statutes precluded the reports from being publicly disclosed or from ultimately being admitted into evidence, the Washington high court ruled that the reports could be discoverable in the widower's case and in a consolidated similar case.[171] Though the United State's Supreme Court ultimately reversed, the potential significance for future electronic discovery disputes is nonetheless evident in the Washington high court's observation that:

> As governments everywhere move from paper and microfiche

[164] *Id.* at *39. One has to wonder about the candor of Defendants' evidence, given that one of their defenses was that the information had already been produced in printouts. If the extraction process were indeed so complicated, then how did Defendants extract the information to produce the printed reports?

[165] *Id.* Mere speculation of another sort doomed another Plaintiff's recent electronic discovery request in *Stallings-Daniel v. Northern Trust Co.*, 2002 U.S. Dist. LEXIS 4024 (N.D. Ill. Mar. 12, 2002). The court denied the employee-Plaintiff's request to use an expert to search company-Defendant's e-mail system to determine whether e-mails produced to her in hardcopy had been altered. The court found that Plaintiff's request "was supported by nothing more than speculation that [D]efendant had somehow altered its e-mails before producing them." 2002 U.S. Dist. LEXIS 4024, at *1-2.

[166] *Jones v. Goord*, 2002 U.S. Dist. LEXIS 8707, at *42.

[167] *Id.* at *37.

[168] *Id.* at *46-47.

[169] *Id.*

[170] *Guillen v. Pierce County*, 144 Wash. 2d 696, 31 P.3d 628 (2001), also available at <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=wa&vol=2001_sc/68535-5&invol=3>, *reversed and remanded,* 537 U.S. 129 (2003) (evidentiary privileges construed narrowly; interpreting federal statute to validly protect from disclosure to tort plaintiffs any information collected for statutory purpose of seeking to receive federal funding for road improvements).

[171] 31 P.3d at 632-33.

> documentation into the age of twenty-first century information technology, public records are increasingly being stored - even created – in digital format, then added to virtual databases that are accessed, in streams of bits and bytes, by vast networks of governmental agencies, often across jurisdictional boundaries.[172]

4. Allocating Compilation and Production Costs

The fact that production of electronic information will result in substantial expense does not necessarily mean that the requesting party will be required to pay the costs of production.[173] In fact, sophisticated companies' protestations as to the burdens of retrieval are increasingly falling on deaf ears.[174] Who pays for the costs of searching, extracting, and producing electronic data depends upon the parties' relative circumstances and how much, if at all, the production would also benefit the responding party.[175] In balancing such factors in various factual contexts, federal district court cases have reached disparate outcomes. Significantly, a very recent decision's new standard appears to restrict a responding party's attempt to shift retrieval costs to the requesting party.[176]

Some decisions have shifted to the requesting party the costs of compiling and

---

[172] *Id.* at 646. For a discussion of the impacts of efiling and egovernment*, see generally* William A. Fenwick & Robert D. Brownstone, "*Efiling: What Is It? What are its Implications?*" 19 SANTA CLARA COMPUTER & HIGH TECH L.J. 181 (2002), available at <http://www.fenwick.com>.

[173] *In re Brand Name Prescription Drugs Antitrust Lit. ("Ciba")*, 1995 U.S. Dist. LEXIS 8281, 1995 WL 360526 (N.D. Ill. June 15, 1995) (class action defendants included Ciba-Geigy Corp.), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/cost/brandname.html>.

[174] "Upon installing a data storage system, it must be assumed that at some point in the future one may need to retrieve the information previously stored." *Kaufman v. Kinko's, Inc.*, Civ. Action No. 18894-NC, *slip op.* at 5 (Del. Ch. Apr. 16, 2002) ("[t]hat there may be deficiencies in [a] retrieval system (or inconvenience and cost associated with the actual retrieval) cannot be sufficient to defeat an otherwise good faith request to examine relevant information (or information likely to lead to the discovery of admissible evidence"), available for purchase at <http://www.virtualdocket.com/>. Moreover, " 'if a party chooses an electronic storage method the necessity for a retrieval program or method is an ordinary an foreseeable risk.' " *Id.* at 4 n.2 (quoting *In re Brand Name Prescription Drugs Antitrust Litig.*, 1995 U.S. Dist. LEXIS 8281, *2, 1995 WL 360526 (N.D. Ill. June 15, 1995), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/cost/brandname.html>).

[175] *Anti-Monopoly*, 1995 U.S. Dist. LEXIS 16355, at *2 (potential factors include whether: " amount of money is . . . inordinate and excessive[,] . . . relative expense and burden in obtaining the data would be greater to the requesting party as compared to the responding party, and . . . responding party will benefit to some degree in producing the data in question"). *See also Rowe Entertainment, Inc. v. William Morris Co*., 205 F.R.D. 421, 2002-1 Trade Cas. (CCH) P73, 567 (S.D.N.Y. 2002) (applying eight-factor balancing approach; granting Defendants' motion for protective order to extent Plaintiffs would bear costs of production – though Defendants would continue to bear expense of reviews for privileged or confidential material).

[176] *Zubulake v. UBS Warburg LLC*, 2003 U.S. Dist. LEXIS 7939 (S.D.N.Y. May 13, 2003) ("*Warburg*"), available at <http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/03-04265.PDF>.

producing electronic information.[177] In one case, the *Linnen v. A.H. Robins* fen/phen class action, the court ordered the responding party to bear the expenses of back-up tape restoration.[178] Yet, the *Linnen* judge reserved a ruling on fees and costs associated with additional pertinent depositions sought by the requesting party until after the parties had an opportunity to evaluate information generated from the back-up tapes.[179] In another case, where the responding entities were non-parties, the court seemed to be more sensitive to the assertion that compliance would be overly burdensome.[180]

Other decisions have declined to remove the cost burden from the shoulders of the responding party.[181] In one such instance, a court mandated payment of all expenses unnecessarily incurred because of Defendant's inaccurate disclosure of its computer capabilities.[182] In another case, a federal antitrust class action, Plaintiffs sought to compel one of the defendants, Ciba-Geigy Corp. ("Ciba"), to produce responsive, computer-stored

---

[177] *See Byers v. Illinois State Police*, 2002 US Dist. LEXIS 9861, * 38 (N.D. Ill. June 3, 2002) (in employment discrimination action, "[r]equiring the plaintiffs to pay part of the cost of producing the [archived] e-mails [from one individual Defendant to Plaintiff] will provide them with an incentive to focus their requests"); *Simon Property Group L.P. v. MySimon, Inc.*, 194 F.R.D. 639, 641 (S.D. Ind. 2000), supp'd by, 2000 U.S. Dist. 8953 (S.D. Ind. June 15, 2000); *Northwest Airlines, Inc. v. Local 2000 Int'l Brotherhood of Teamsters*, Civ. Action No. 00-08, Order, at 3 ¶ 5 (D. Minn. Feb. 2, 2000); *Playboy Enters., Inc. v. Welles*, 60 F. Supp. 2d 1050, 1054-55 & n.6 (S.D. Cal. 1999), *aff'd in part & rev'd in part on other grounds*, 279 F.3d 796 (9th Cir. 2002).

[178] *Linnen*, 1999 Mass. Super. LEXIS 240, at *22-23 (imposing all fees and costs associated with e-mail discovery issue, including depositions of IT representatives, in light of Defendant's: lack of cooperation in responding to requests on e-mail issues; its denial of existence of back-up tapes; and its delay in informing Plaintiff of existence of archived back-up tapes).

[179] In dicta, the court stated that:

> [I]t certainly would be fair to require [Defendant] to bear the costs associated with the retaking of any depositions previously conducted by the Plaintiffs as well as any appropriate new depositions. Where the necessity of engaging in further depositions stems from the Defendant's delay in producing documents requested, at a minimum, over a year ago, then the defendant must shoulder the costs attendant upon such a delay.

Id. at 20.

[180] *Braxton v. Farmer's Ins. Group*, 2002 U.S. Dist LEXIS 18085, *7 (N.D. Ala. Sep. 13, 2002). In *Braxton*, a plaintiff served subpoenas requesting the production of e-mail by non-party insurance agents affiliated with Defendant. Defendant moved to quash, arguing that compliance would impose a substantial burden on the non-party agents. *Id.* Acknowledging that burden, the court refused to compel production absent a showing by Plaintiff that production of all such e-mail and other documents from Defendant itself would have been insufficient. *Id.*

[181] *See, e.g., Bills v. Kennecott Corp.*, 108 F.R.D. 459 (D. Utah 1985) (declining to shift from Defendant/employer to Plaintiffs/employees, given amount of expenses and relative abilities to bear cost).

[182] *GTFM, Inc. v. Wal-Mart Stores*, 2000 U.S. Dist. LEXIS 3804, *7-10 (S.D.N.Y. Mar. 30, 2000), enforced, 2000 U.S. Dist. LEXIS 16244 (S.D.N.Y. Nov. 9, 2000) (ultimately awarding requesting party $109,753.81 in expenses and attorney fees). In *GTFM* the court also factored in Defendant's poor track record on compliance with discovery requests in litigation generally, not just in that particular case.

e-mails at its own expense.[183] Ciba objected, arguing that the request was overly broad and burdensome, and that Plaintiffs should bear the retrieval costs.[184] Ciba estimated it had the equivalent of at least 30 million pages of e-mail data stored on back-up tapes, and that it would cost from $50,000 to $70,000 to search for responsive e-mails, eliminate duplicates, and format the messages. The court declined to impose on Plaintiffs that cost because it resulted from Ciba's record-keeping scheme and its choice of electronic storage.[185] The court only required Plaintiffs to pay $0.21 per page for the e-mails that they selected for copying; and it also ordered them to narrow the scope of their electronic information request.[186]

The landscape on the cost-shifting issue shifted greatly[187] last month due to the new multi-factor test pronounced in *Zubulake v. UBS Warburg LLC*, 2003 U.S. Dist. LEXIS 7940 (S.D.N.Y. May 13, 2003) ("*Warburg*")[188] by Judge Shira A. Scheindlin. The *Warburg* grant of a motion to compel arose in an employment litigation entailing claims for gender discrimination and illegal retaliation. The court criticized prior decisions as having engaged in cost-shifting analysis as a knee-jerk reaction, based on a faulty "assum[ption] that an undue burden or expense may arise simply because electronic evidence is involved."[189] As a matter of policy, *Warburg* noted that "cost-shifting may effectively end discovery, especially when private parties are engaged in litigation with large corporations. As large companies increasingly move to entirely paper-free environments, the frequent use of cost-shifting will have the effect of crippling discovery in discrimination and retaliation cases."[190]

As its threshold issue, the *Warburg* decision divided the world of electronic information into two distinct broad categories:

1) "[D]ata that is kept in an ***accessible*** format, [as to which] the usual rules of discovery[191] apply: the responding party should pay the costs of producing responsive

---

[183] *In re Brand Name Prescription Drugs Antitrust Litig.*, 1995 U.S. Dist. LEXIS 8281, *2, 1995 WL 360526 (N.D. Ill. June 15, 1995), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/cost/brandname.html>.

[184] *Id.* at *1.

[185] *Id.* at *2.

[186] *Id.* at *8.

[187] Landon Thomas, "*A Ruling Makes E-mail Evidence More Accessible,"* N.Y. Times (May 17, 2003).

[188] *Zubulake v. UBS Warburg LLC*, 2003 U.S. Dist. LEXIS 7939 (S.D.N.Y. May 13, 2003) ("*Warburg*"), available at <http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/03-04265.PDF>.

[189] *Id.* at * 27. By way of example, *Warburg* described a predecessor decision as follows: "*Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, . . . 2002 WL 246439, at *3 (E.D. La. Feb. 19, 2002) (suggesting that application of [multi-factor cost-shifting analysis] is appropriate whenever 'a party . . . contends that the burden or expense of the discovery outweighs the benefit of the discovery')." *Id. at *27* n.48.

[190] *Warburg*, 2003 U.S. Dist. LEXIS 7939, *26.

[191] *See* Fed. R. Civ. P. 26-37, quoted and discussed at length in *Warburg*, 2003 U.S. Dist. LEXIS 7939, *17-20.

data."[192]

2) "Electronic data [that] is relatively ***inaccessible***, such as in backup tapes," as to which a "court should consider cost-shifting."[193]

Warburg then modified the multi-factor test espoused by a prior Southern District of New York decision.[194] Under the new *Warburg* approach, once a small sample of inaccessible data has been produced,[195] "in conducting the cost-shifting analysis, the following factors should be considered, weighted more-or-less in the following order":[196]

1. The extent to which the request is specifically tailored to discover relevant information;

2. The availability of such information from other sources;

3. The total cost of production, compared to the amount in controversy;

4. The total cost of production, compared to the resources available to each party;

---

[192] *Warburg*, 2003 U.S. Dist. LEXIS 7939, *49 (emphasis added). According to *Warburg,* the three subsets of "accessible" media, "listed in order from most accessible to least accessible," are:

a) "Active, online data," such as hard drives;

b) "Near-line data," such as optical disks.

c) "Offline storage/archives . . . [,] lack[ing] 'the coordinated control of an intelligent disk subsystem,' and is, in the lingo, JBOD ("Just a Bunch of Disks").

Id. at 30-31.

[193] *Id.* at *49-50. According to *Warburg,* the two subsets of "inaccessible" media, in order from more accessible to less accessible," are: a) "[b]ackup tapes;" and b) "[e]rased, fragmented or damaged data." *Id.* at 31-32.

[194] *Rowe Entertainment, Inc. v. William Morris Co*., 205 F.R.D. 421, 2002-1 Trade Cas. (CCH) P73, 567 (S.D.N.Y. 2002) (upon applying eight-factor balancing approach, ordering Plaintiffs to bear costs of production and Defendants to continue to bear expense of reviews for privileged or confidential material). The *Warburg* test eliminated two of the *Rowe* factors, namely "the specificity of the discovery request" and "the purposes for which the responding party maintains the requested data." *Id.* at *40-41. The "purposes" concept was eclipsed by Judge Scheindlin's accessibility/inaccessibility demarkation: "Whether the data is kept for a business purpose or for disaster recovery does not affect its accessibility, which is the practical basis for calculating the cost of production." *Id.* at 41. The court even noted that, in "certain limited instances where the very purpose of maintaining the data will be to produce it to the opposing party. . . . cost-shifting would not be applicable in the first place; the relevant statute or rule would dictate the extent of discovery and the associated costs." *Id.* at *42 & nn. 69-70 (citing SEC requests for "communications sent by [a] broker or dealer . . . relating to his business as such" because "such communications must be maintained pursuant to SEC Rule 17a-4, [17 C.F.R. § 240.17a-4]."

[195] *Warburg*, 2003 U.S. Dist. LEXIS 7939 at *50.

[196] *Id.*

5. The relative ability of each party to control costs and its incentive to do so;

6. The importance of the issues at stake in the litigation; and

7. The relative benefits to the parties of obtaining the information.[197]

In *Warburg*, this new test was applied to a pertinent set of 94 back-up tapes that had previously been identified as responsive. The court ordered Defendant to produce at its own expense: "*all* responsive e-mails that exist on its optical disks or on its active servers[;] . . . and responsive e-mails from any *five* back-up tapes selected by [*Plaintiff*]."[198] The court also ordered Defendant to "prepare an affidavit detailing the results of its search, as well as the time and money spent. After reviewing the contents of the backup tapes and UBS's certification, the Court will conduct the appropriate cost-shifting analysis."[199]

III. PRACTICAL LITIGATION TIPS REGARDING ELECTRONIC DISCOVERY

A. Tips for Requesting Electronic Information from the Other Side

1. Overview/Strategy

The amount of time and attention you devote to seeking discovery of electronic data should depend upon the size of the case, the matters at issue, and the time and resources available for the case. Early in the case (and if possible before the case is filed), you should think about what types of electronic information are likely to exist and are needed to prove the case. Before asking for the production of electronic data, such as back-up tapes and deleted files, weigh the costs against the potential benefits. Back-up tapes, for example, must be restored and searched for responsive information; depending upon the number of tapes, it can entail a costly and time-consuming process. If the circumstance justifies requesting information in electronic form, obtain expert assistance in framing and justifying the request. Keep in mind that the opponent will likely ask your client for reciprocal information, if both parties rely on electronic record keeping and processing systems. Even if not served initially, the request could come later. If you plan to press an opponent to preserve and produce a broad amount of electronic information, make sure your client is doing the same and that the collection and preservation efforts are thorough, adequate, and above reproach.[200]

---

[197] *Id.*

[198] *Id.* at *50-51.

[199] *Id.* at *51.

[200] *See, e.g., Procter & Gamble Co. v. Haugen*, 179 F.R.D. 622, 631-32 (D. Utah 1998) (imposing sanctions on Plaintiff for failure to preserve corporate e-mails of "five individuals that [Plaintiff] had itself identified as having relevant information" when, earlier in case, Plaintiff had insisted that opposing party preserve all its corporate e-mail communications until relevant material could be extracted), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/process/procterandgamble.html>, *aff'd & rev'd on other grds.*, 222 F.3d 1262 (10th Cir. 2000).

2. Preservation Requests and Orders

If electronic information is important, promptly notify the other side of your intent to request it. Early in the case, you should consider sending a letter to opposing counsel reminding him or her of the obligation to preserve evidence, including electronic data, and delineating the categories of electronic evidence your client will be seeking (e.g., e-mails, databases, spreadsheets, back-up tapes and transaction records). Elucidate your side's expectations and desires.

A powerful tool in the effort to obtain electronic information is a preservation order. The duty to preserve evidence exists independently of a court order.[201] Yet, to highlight that obligation, to set forth the ground rules, and to provide sharper teeth, you should ask the court to enter a preservation order specifically identifying electronic information.[202] The absence of a court order may narrow the scope of the available sanctions should evidence destruction ensue.[203]

In one case Defendant moved for sanctions based on Plaintiff *Procter & Gamble's* (P&G) alleged destruction of e-mail communications.[204] In the absence of a preservation

[201] The duty to preserve is not necessarily contingent on an existing court order. *See West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999) ("[e]ven without a discovery order, a district court may impose sanctions for spoliation, exercising its inherent power to control litigation" (citing *Chambers v. Nasco, Inc*., 501 U.S. 32, 43-43 (1991)).

[202] For some reported cases containing examples of preservation orders, *see Linnen*, 1999 Mass. Super. LEXIS 240, at *23-24 (initial ex parte order mandated "all necessary steps to assure that . . . employees, agents, accountants and attorneys refrain from discarding, destroying, erasing, purging or deleting any such documents including . . . computer memory, computer disks, data compilations, e-mail messages sent and received and all back-up computer files or devices, including . . . electronic, optical or magnetic storage media"); *Smith v. Texaco Inc.*, 951 F. Supp. 109 (E.D. Tex. 1997) (in employment discrimination class action, temporary restraining order prohibited Defendants from moving, altering or deleting any potentially pertinent electronic records; court altered TRO to permit modifications in ordinary course of business and deletion of documents if hardcopies retained), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/smith.html>, *rev'd on other grounds*, 263 F.3d 594 (5th Cir. 2001).

See also In re Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598, 600 (D.N.J. 1997) (entering order at beginning of case that all parties "preserve all documents and other records containing information potentially relevant to the subject matter of this litigation"); *In re Infant Formula Antitrust Litig.*, 1991 U.S. Dist. LEXIS 202532, *2-3, 1991-2 Trade Cas. (CCH) ¶ 69,553 (N.D. Fla. Aug. 16, 1991) (stipulated order imposing preservation obligation regarding "any relevant document or other relevant item, " defined broadly to encompass "all mechanical and electronic sound records or transcripts thereof, any retrievable data whether carded, taped, coded, electrostatically, electromagnetically or otherwise, and other data compilation from which information can be obtained").

[203] *Linnen*, 1999 Mass. Super. LEXIS 240, at *30-31 (declining to award monetary sanctions for Defendant's spoliation, which ran afoul of informal understanding that had replaced withdrawn order); see also *Procter & Gamble Co. v. Haugen*, 179 F.R.D. 622, 631-32 (D. Utah 1998), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/process/procterandgamble.html>, *aff'd in part & rev'd in part on other grounds*, 222 F.3d 1262 (10th Cir. 2000).

[204] *Procter & Gamble Co. v. Haugen*, 179 F.R.D. 622, 631-32 (D. Utah 1998), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/process/procterandgamble.html>, *aff'd in part & rev'd in part on other grounds*, 222 F.3d 1262 (10th Cir. 2000).

order, P&G had responded to Defendant's requests for production by searching its e-mail databases for responsive evidence and then deleted non-responsive data. Defendant challenged the adequacy of those searches, claiming that responsive evidence had been deleted. The court concluded that it could not fairly judge the adequacy of Plaintiff's searches, with the exception of the deletions of the e-mail of five individuals whom Plaintiff itself had identified as having relevant information.[205] The court explained:

> [W]hile the duty to preserve evidence exists independently of court order, a court order would have delineated the scope of P&G's duties, provided clear evidence that P&G was on notice of the relevance of the e-mail communications, and furnished a standard by which this court could judge the adequacy of P&G's production efforts.[206]

In another case, the court required "all parties to preserve the integrity of all computers . . . at issue . . . without any spoilation [sic] of any information contained therein."[207] Elaborating on that mandate, the judge stated: "[I]f it's 'don't push the delete button' or if it's 'don't change the C drive' or 'don't pull the plug at the wrong time' or 'don't take a sledge hammer to it,' I don't want it spoiled in any way, okay, so don't limit [the preservation order's language]."[208]

Consider expedited or early depositions of the opposing party's employees who are most knowledgeable about the opponent's information technology uses and systems. Such early discovery should eliminate some of the types of delay and vagueness arguments successfully raised by the party opposing discovery in *Goord*.[209]

3. Considerations Particular to Electronic Information

a. Specifically Request All Desired Types of Items

To request all needed forms of electronic information, make sure your definition of documents particularizes various forms of electronic media.[210] Also, do not merely rely upon a broad definition of "documents." Such broad definitions are commonplace, and the opposing party may overlook them. If, for example, you desire e-mails, spreadsheets and databases relating to specified topics, then specify those items in the requests

---

[205] *Id.*

[206] *Id.* at 631.

[207] *Illinois Tool Works, Inc. v. Metro Mark Prods., Ltd.*, 43 F. Supp. 2d 951, 954 (E.D. Ill. 1999).

[208] *Id.*

[209] 2002 U.S. Dist. LEXIS 8707, at *28-29, 46-47.

[210] *See, e.g., Linnen*, 1999 Mass. Super. LEXIS 240, at *4 n.3 ("document" defined to include "any record or compilation of information of any kind or description however made, produced, or reproduced, or stored whether by hand or by any electronic, photographic, magnetic, optical, mechanical, computer or other process or technology"); *R.S. Creative, Inc. v. Creative Cotton, Ltd.*, 75 Cal. App. 4th 486, 489, 89 Cal. Rptr. 2d 353 (1999) ("definition of 'document' in deposition notice included computer tapes, discs and any information stored in a computer").

themselves.[211] That way, there can be no mistake as to what your client seeks. In addition, courts do not look favorably on unduly broad and burdensome definitions. For example, one court denied a motion to compel because "Plaintiffs are not entitled to unbridled access [to D]efendants' computer system or to canvass all of Defendants' debtor files."[212]

Though one should be as proactive as possible from the get-go, occasionally, in the interests of justice, a court will modify an overly broad discovery request. In one 2002 case,[213] Defendants claimed that the discovery request for "all summary documents" (including electronic data) was overbroad.[214] Plaintiffs alleged that Defendants had constructed a rebuttal report based on a couple of million entries it had deleted from a database and thus deliberately withheld. "The data was not produced by Defendants until after [Defendants'] rebuttal report was submitted, after Plaintiff's expert report had been submitted and Plaintiffs' expert had been deposed."[215] The court found that Defendant "should have produced the disputed database."[216] After considering a range of responses (including sanctions, which it declined to impose), the court decided to "allow Plaintiffs the opportunity to respond to Defendants' rebuttal expert report [and to deny] Defendants . . . the opportunity to reply to Plaintiffs' response to the withheld information."[217]

In a dispute between competing software companies regarding allegedly improper copying and use of proprietary source code, Plaintiff sought production of the entire source code for each of Defendant's products from the previous three and one-half years.[218] Plaintiff also requested copies of all hard drives that had access to the server from which

---

[211] At least until such time as judges are more comfortable with the concept of electronic information, the prospect of defeating a motion for a protective order as well as the success of any "meet and confer" conference will be dependent on the specificity of the request for electronic information.

A large number of judges reject out of hand a request for "all" of anything. Rather than attempting to encompass "electronic information" in the definition of "document," in some situations requesting counsel may want to differentiate hardcopies of information from copies of electronic information.

[212] *Van Westrienen v. Americontinental Collection Corp.*, 189 F.R.D. 440, 441 (D. Ore. 1999). *See also Sabouri v. Ohio Bureau of Employment Servs.*, 2000 WL 1620915, *5 (S.D. Ohio Oct. 24, 2000) ("[a]lthough [P]laintiff is entitled to view files that relate to him or to the claims or defenses asserted in this action, he has no right to rummage through the computer files of the Defendants").

[213] *DeLoach v. Philip Morris Cos.* 206 F.R.D 568 (M.D.N.C. 2002).

[214] When Defendant claimed Plaintiff had a responsibility to contact opposing counsel to discuss the missing data, the court noted that Plaintiff did not know any data was missing until Defendants filed their expert rebuttal report. *DeLoach v. Philip Morris Cos.*, 206 F.R.D 568, 573 (M.D.N.C. 2002). "[T]he disputed data was readily available from [Defendants'] database, required no additional preparation, and was obviously relevant enough that Defendants saw fit to provide it to [its expert]." *Id.* at 574.

[215] *Id.* at 573. Defendant then deleted more than two million entries (without informing Plaintiff of the deletion) and provided Plaintiff with "the single item that was specifically and unambiguously requested." *Id.*

[216] *Id.* at 574.

[217] *Id.*

[218] *Symantec Corp. v. McAfee Assocs., Inc.*, 1998 U.S. Dist. LEXIS 22591, *10 (N.D. Cal. Aug. 14, 1998).

the information at issue was purportedly copied.[219] The court ruled that "[p]roduction of this magnitude would be unduly burdensome to [Defendant], both in terms of volume and in terms of the proprietary nature of the information sought."[220]

b. "Meet and Confer" Negotiations

It is a good practice to discuss with the other side the logistics of electronic discovery early in a litigation. Especially in an action in which electronic information is likely to be significant, such a discussion is likely necessary to assure compliance with Fed. R. Civ. P. 26(f). Rule 26(f) provides in pertinent part that "the parties must, as soon as practicable and in any event at least 21 days before a scheduling conference is held or a scheduling order is due under [Fed. R. Civ. P.] 16(b), confer . . . to develop a proposed discovery plan." As one federal district court judge pointed out last year:

> In the electronic age, this [Rule 26(f)] meet and confer should include a discussion o[f] whether each side possesses information in electronic form, whether they intend to produce such material, whether each other's software is compatible, whether there exists any privilege issue requiring redaction, and how to allocate costs involved with each of the foregoing.[221]

As part and parcel of "meet and confer," you might try to informally obtain information about your opponent's computer system, including its functionality, breadth, scope, and number of users. Consider methods to search for responsive information. Some e-mail systems have search functions that could expedite the process; also, there may be software to help search databases. It would be useful to obtain a copy of the opponent's document retention or records management policy and also a copy of its e-mail policy. In addition, hardcopy documents may reveal information about the opponent's computer system, including the use of third party software, system flow charts, file naming conventions, e-mail programs and the like.[222]

---

[219] *Id.*

[220] *Id.*

[221] *In re Bristol-Myers Squibb Securities Litig.*, 205 F.R.D. 437, 443-45 (D.N.J. 2002) ("denying Defendants' [request] for . . . full reimbursement for paper copying costs" where Defendants had "dumped" more than three million pages on Plaintiffs; also denying "Defendants' [request] . . . that the Plaintiffs pay one-half the costs of scanning documents [i]nto electronic form in favor of requiring Plaintiffs "to pay the nominal cost of duplicating compact discs").

See also "[G]ood faith attempt at an informal resolution" required by, among other provision, California Code of Civil Procedure §§ 2017(c)-(d), 2025(g), (o), 2031(f), (m), 2033(e), (l); Cal. Civ. Proc. Code § 2017(e), available at <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=ccp&group=02001-03000&file=2016-2036> ("[p]ursuant to noticed motion, a court may enter orders for the use of technology in conducting discovery in cases designated as complex"). *See generally* Richard E. Best (SF Super. Ct. Discovery Commissioner), California Discovery, "*Meet and Confer*" (1999). <http://californiadiscovery.findlaw.com/MEET_AND_CONFER_WEB.htm#STATUTES>.

[222] A discovery issue beyond the scope of this paper is the ability to take depositions over the Internet. Fed. R. Civ. P. 30(b)(7) expressly provides that "[t]he parties may stipulate in writing or the court may upon motion order that a deposition be taken by telephone or other remote electronic means." *See also* Vt. R. Civ. P. 30(b)(7) (same). "Increasingly, parties are conducting depositions by remote electronic means due to

A cautionary tale as to the pitfalls of delaying discussion of the logistics of computer discovery emerges from *Danis v. USN Communications, Inc.*[223] There, the court criticized the parties for their failure to communicate or to gain "a complete mastery of what types of documents were generated by [Defendant] in the ordinary course of business, how they were used, or their significance."[224]

c. Details Of the Opponent's Computer System

Specific, well-thought-out and thorough requests for electronic data should be made as early in the litigation as possible. Thus, to prevent the kind of prejudicial delay that doomed the *Goord* Plaintiffs, you should follow the wise course of initially serving interrogatories, and then following up with a document request and/or a deposition notice accompanied by a list of requested documents and data. Interrogatories can be used to obtain preliminary information about the layout of an opponent's computer system, including hardware, software, software applications, back-ups, e-mail and voicemail administration, and similar issues. When follow-up questions flow from the interrogatory responses, and/or when the location and/or amount of computer data are important, you can then notice the deposition(s) of person(s) with knowledge, such as the Information Technology (IT) Director. In federal court Rule 30(b)(6) depositions can be used to avoid using up many of the allowed depositions.[225] Some outlines of sample questions for IT

---

improved technologies and both time and financial constraints, particularly when the nature of the testimony or other factors do not require the personal attendance of the attorney. Effective 2002, such practices are expressly authorized by [California] statute." Richard E. Best (San Francisco Superior Court Discovery Commissioner), "*Virtual Discovery: Conducting Discovery in a Web Centric Environment*" <http://californiadiscovery.findlaw.com/Internet_Discovery.htm#TELE_DEPO> (citing Cal. Civ. Proc. Code § 2025(h)(3) ("[a] person may take, and any person other than the deponent may attend, a deposition by telephone or other remote electronic means")).

In addition to Vermont and California, at least 15 other "states have rules governing video depositions, according to the National Center for State Courts." Rebecca Porter, "*The Next Step: Taking Depositions Online*" (Trial Magazine Aug. 2001). <http://i-dep.com/news/trial_8-01.asp>. Some vendors that apparently provide Internet deposition services include I-DEP <http://i-dep.com/examine/ideps.asp>, Depocast.com <http://www.depocast.com/> and several others whose home pages are linked off of Richard E. Best's "*Web Sites re Web Centric Discovery*." <http://californiadiscovery.findlaw.com/Internet_Discovery.htm#WEBSITES>. By using some real time deposition transcript services, all parties to a deposition can view the transcript of the testimony as it is being given, in addition to seeing it on video or hearing it via conferencing telephone hookups.

[223] 2000 U.S. Dist. LEXIS 16900 (N.D. Ill. Oct. 23, 2000), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/danis.html>.

[224] *Danis*, 2000 U.S. Dist. LEXIS 16900, at *13-14. *See also Jones v. Goord*, 2002 U.S. Dist. LEXIS 8707, at *48 (S.D.N.Y. May 16, 2002) (denying electronic discovery request deemed "belated" and "speculative" due to six year delay and lack of a specific - let alone expert-based - discovery plan).

[225] A 30(b)(6) deposition counts as only one deposition regardless of the number of persons designated by a party serving a 30(b)(6) notice. Thus, 30(b)(6) depositions are outside the scope of the "leave of court" a party must obtain to exceed the ten depositions limit set by Fed. R. Civ. P. Rule 30(a)(2)(A), and by Fed. R. Civ. P. Rule 31(d)(2)(A) ("Deposition Upon Written Questions").

30(b)(6) depositions are available on the web.[226]

A deposition would be particularly useful if, for example, the other side is resistant to the notion of electronic discovery and/or you have reason to believe all responsive electronic information has not been produced in response to a prior discovery request. More broadly, however, some courts have expressly approved the use of depositions to learn about a party's computer system and electronic information.[227]

Third parties may possess electronic information of a party. For example, a third party may administer a company's Internet or intranet service, and/or may possess back-ups of e-mails. In the era of increasingly used Application Service Providers (ASP's) and multi-faceted web services,[228] this consideration is now even more important than ever. A third party consultant may have been used to administer system back-ups, and may thus possess copies of back-up tapes. In either event, you might consider subpoenaing electronic information in the possession of the third party.[229]

The existence of an alternative source can severely undercut a motion to compel production of electronic data from a party. For instance, one court found that the prejudice to Plaintiffs resulting from Defendants' failure to produce information from a database was mitigated by Plaintiffs' ability to obtain that information from a third party.[230] And another court denied an emergency *ex parte* application for a temporary restraining order to prevent anticipated destruction and concealment of computer files, ruling that "Plaintiffs' own complaint and . . . application reveal[ ] ample alternative sources of proof."[231]

---

[226] *See, e.g.,* Paul French, "Unlocking E-Evidence: Know How to Discover Computerized Information," L.A. D.J. (Aug. 13, 2002), available at <http://www.dataforensics.com/PDFS/ladj_1.pdf> and also fleshed out at <https://www.technolawyer.com/member/archivehome.asp> as "TechnoFeature: E-Discovery Through FRCP 30(b)(6) Depositions," TechnoLawyerArchive (Nov. 19, 2002); Richard A. Lazar, Esq., "*The Guide to Electronic Discovery*," 64-73 (2002) ("Fios Guide") ("appendix C: sample FRCP 30(b)(6) deposition questions, available at <http://www.fiosinc.com/simplified/register.html>. *Cf.* Fios Guide 51-63 ("appendix b: sample electronic discovery interrogatories and requests for production").

[227] *See In re Carbon Dioxide Indus. Antitrust Litig.*, 155 F.R.D. 209, 213 (M.D. Fla. 1993) (denying Defendants' motions to quash Fed. R. Civ. P. 30(b)(6) notices for depositions regarding their computer systems; those depositions were "to identify how data is maintained and to determine what hardware and software is necessary to access the information[,] are preliminary depositions necessary to proceed with merits discovery."). *But see Lawyers Title Ins. Corp. v. United States Fidelity & Guaranty Co.*, 122 F.R.D. 567, 570 (N.D. Cal. 1988) (denying request for information about a party's computer system, absent evidence that the party had failed to respond to discovery requests adequately and in good faith).

[228] For a discussion of web services, see Questra, "*Web Services in Embedded Systems*" (White Paper July 2001). <http://www.questra.com/literature/white_papers/web_services_wp.pdf>.

[229] Third party services are sometimes use for on-line meetings and remote presentations. Records of such services can be valuable in proving such meetings occurred and providing a basis for inquiring about what occurred at such meetings.

[230] *Danis*, 2000 U.S. Dist. LEXIS 16900, at *78. *See also Mathias v. Jacobs*, 197 F.R.D. 29, 37 (S.D.N.Y. 2000), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/mathias.html>, *vacated*, 167 F. Supp. 2d 606 (2002).

[231] *Adobe Systems, Inc. v. South Sun Prods., Inc.*, 187 F.R.D. 636, 643 (S.D. Cal. 1999).

4. Parameters of Seeking Court Intervention

If you cannot reach a compromise and the other side is refusing to produce electronic information, then take action promptly. Especially in this era of XML-generated websites and database proliferation, electronic data is rarely static. Such data is dynamic, and is constantly modified, deleted and/or compromised. If there are technical issues in dispute, carefully consider the information and education the court will need to decide those issues. If the existence of the requested information is at issue, marshal your evidence to show that the information exists and that your request is not a fishing expedition. Carefully limit your requests to information you really need. In addition, to help reduce the time and effort involved, consider practical limits on searches (*e.g.*, date restrictions, limitations to certain search terms and/or, if appropriate, limitations to computers used by a reasonable list of pertinent individuals). For voluminous electronic databases, the requesting party might ask for searches of the databases using specific key word searches. If the parties cannot agree upon the nature and scope of those searches, let alone their key words, they can ask the court to resolve the impasse.[232]

If a Defendant proves uncooperative in discovery, a court may be more receptive to a Plaintiff's request for extensive electronic discovery.[233] For instance, in *Tulip*,[234] a patent case, the court granted Plaintiff's customized discovery request that Defendant make its senior executives' e-mail records available, after having an opportunity to address privilege and confidentiality concerns.[235] Plaintiff's proposed procedure was deemed "fair, efficient, and reasonable."[236] Defendant had to "provide the e-mails from the hard disks of the identified executives in electronic form to [Plaintiff's consultant,]" who would "search the e-mails based on an agreed upon list of search terms."[237] Plaintiff was directed to give

---

[232] *See, e.g., Procter & Gamble*, 179 F.R.D. at 632 (of 25 proposed search terms allowed by magistrate judge: certain word searches were too narrow, leaving out discoverable and relevant subjects; and another was overly broad, thus reaching into non-discoverable matters or yielding so much information as to be "unwieldy for any purpose legitimately within the current framework of the litigation"). *See also Alexander v. FBI*, 194 F.R.D. 316 (D.D.C. 2000) (in "Filegate" case, narrowing Plaintiff's request to search more than 50 individuals' e-mail via 37 proposed search terms to 33 individuals via 20 search terms).

[233] *See Tulip Computers Int'l B.V. v. Dell Computer Corp.*, 2002 U.S. Dist. LEXIS 7792 (D. Del. Apr. 30, 2002), also available at <http://www.ded.uscourts.gov/RRM/Opinions/Apr2002/00-981.pdf>.

[234] *Id.*

[235] *Id.* at *18-19. The court's rationale was that:

> The history of [Defendant's] failures to cooperate in the discovery process - and its sweeping but inaccurate positions that [Plaintiff] would never find certain documents that [Plaintiff], through persistence and diligence, later uncovered - counsel in favor of awarding [Plaintiff] some relief that allows them to ascertain for themselves whether [Defendant's] representations that all responsive documents have been produced are accurate. Moreover, counsel for [Defendant] could not represent to the court that it has thoroughly searched these e-mail records for responsive information.

Id. at *19.

[236] *Id.*

[237] *Id.*

Defendant a list of e-mails containing those terms, but was not to read the e-mails until Defendant had an opportunity to review them to ensure that privilege and confidentiality concerns were not compromised.[238]

A court may also partially grant a request for information stored in a database. In a racial discrimination class action, Plaintiffs – all African American women – were searched by Customs following their arrival at Chicago's O' Hare International Airport on international flights.[239] To support their various claims, Plaintiffs sought to discover "the names and addresses of passengers included in [one of four] computer database[s] . . . provided during [previous] discovery."[240] Plaintiffs contended that they needed additional information about persons who were searched by Customs officials but not arrested or subject to seizure of objects (a "Negative Search"). Plaintiffs asserted that the other data was needed for "certain statistical analysis."[241] Plaintiffs also sought to contact a sampling of nonparty passengers to interview them about their Customs treatment. The court ordered Defendants to "provide [passengers'] names, birth dates, and addresses" subjected to Negative Searches, but forbid all parties from "contact[ing] any of the nonparty passengers disclosed in any of the computer databases."[242]

5. Assessing the Adequacy of Opponent's Electronic Production

Test the adequacy of your opponent's search efforts and production. At a deposition, ask the witness whether he or she:

- searched his or her computer and to delineate the types of information stored thereon;
- was instructed to preserve information, including electronic information.
- possesses floppy disks, jaz disks, zip disks, flash memory devices and/or CD-ROM's containing pertinent information;
- uses a laptop and/or other home computer for work purposes.

Ask about the configuration of deponent's computer or workstation-- what it is used for and what information is saved to a storage device. Also, inquire to identify all others, such as assistants, secretaries, or other persons, who have retained and still retain the deponent's electronic information.

---

[238] *Id.*

[239] *Anderson v. Cornejo,* 2001 U.S. Dist. LEXIS 2330 (N.D. Ill. March 6, 2001).

[240] *Id.* at *9.

[241] *Id.* at *16.

[242] *Id.* at *24-25.

B. Tips for Responding to Electronic Information Production Requests

1. Respond to Preservation Requests

It is wise to respond promptly to a preservation letter, including your specific objections and inquiring about the basis for the demand. You might consider seeking a protective order if your opponent's requests appear excessive or unreasonable.

2. Advising Client of Duties to Preserve and Communicate

It is advisable to inform your client of the duty to preserve evidence, and to explain the potential categories of discoverable information, including electronic information. Depending upon the size of your client and the circumstances, it may be advisable for a company officer to communicate with the employees about the lawsuit -- as well as the obligation to preserve all forms of information. This communication should outline the categories of documents and other information to be retained.

The request to preserve should be unequivocal, and, if appropriate, should explain the consequences of a failure to preserve, including penalties and sanctions. Such an explanation is even more warranted by virtue of the possibility – noted above in Section II(A)(1)(c) – that a court might hold a corporate officer personally responsible for a corporation's failure to preserve relevant evidence. Down the line, attorneys should follow up with a client's officers and/or administrators to insure that they have understood and followed through with document retention and collection policies, and have advised their fellow employees appropriately.

3. Inventory and Search Your Client's Computer System

Assess your client's computer system. It would be helpful to understand the layout and structure of the computer system, as well as the locations and sources of electronic information. If there are numerous sources of electronic information, you may need to devise a strategy for searching electronic information (on the network and individual hard drives). For organizational purposes and in anticipation of a subsequent dispute, it would be helpful to keep track of your electronic search efforts. You may eventually be pressed to show the steps taken to preserve, collect, and extract responsive information.

Determine the persons who may have discoverable or relevant information. You should search for and preserve the electronic data of the persons who were, or are, involved in the matters at issue, including, for example, persons:

- identified in the pleadings, witness lists, and initial/mandatory disclosures; and
- who may appear as deponents or maybe also as trial witnesses.

In *Procter & Gamble*, monetary sanctions were imposed against Plaintiff for failing to search or preserve the e-mail communications of five key employees whom Plaintiff had

identified as having relevant information.[243] That case serves as a reminder to involve information custodians in the preservation and searching processes. Expect that, when a custodian is deposed, he or she will be asked questions about the efforts undertaken to search for and produce responsive documents.

4. Consider Retaining Back-Up Tapes

Consider whether your client should change its standard back-up routines. Even if back-up tapes have not been specifically requested, consider whether they are called for by document requests (examine the opponent's definition of "documents"). Your client might consider removing back-up tapes from the recycling rotation, to preserve them for the litigation. Each back-up tape will provide a snapshot of the computer system on a given day. In addition, upon a specific request for back-up tapes, you may ultimately need to advise your client whether it should agree to produce them. If your client does not agree to produce such tapes, inform the other side, providing an explanation. If a compromise cannot be reached, ask the court to resolve the dispute.

In some cases, discovery of back-up tapes may be overly burdensome and/or unnecessary. Back-up tapes might be unavailable, or the volume of back-ups may be very large given the size of the company. The expense of restoring, searching, and extracting information from back-up tapes may be excessive compared to the size of the case. If your matter falls into one of those categories, you might pursue a strategy entailing an ongoing thorough search for, and preservation of, pertinent electronic data. Such an approach could minimize or eliminate the need for discovery of back-up tapes.

5. Secure Information; Establish its Authentication Foundation

You will need to lay the foundation for the authenticity of computer records you plan to introduce in evidence, namely that:

- the information has not been changed;
- it is a complete copy;
- it was made by a reliable copying method; and
- the media have been secured (i.e., the original copies have been preserved).

Whether electronic information was produced by your side or received from the other side, you should carefully track not only its sources, but also the methods by which it was obtained. Make write-protected copies of original data. Run anti-virus checks.[244] Store originals in a secure place - i.e., a place of limited and controlled access – to avoid

---

[243] *Procter & Gamble*, 179 F.R.D. at 632 (such failure "constitute[d] a sanctionable breach of P&G's discovery duties[;] P&G's own identification of these individuals belies any possible claim that P&G was not on notice that their e-mail communications would be relevant").

[244] Donald Searles, "Essentials of Electronic Discovery: What Every Practitioner Must Know," (Cal. CEB PowerPoint presentation March 2002).

the possibility of data corruption via alteration or destruction.[245] Be conscious of the impact of stipulated or court-ordered protective procedures.

6. Considerations Regarding Copying or Inspecting Hard Drives

If the other side wishes to search a hard drive or copy it, first consider whether it has a legitimate, well-founded basis for doing so:

- Is the request premature?
- Is there a particular reason for the search?
- Are there less burdensome ways to address the requesting party's concerns and its rationale for request?

If you and your client are amenable to such a search, try to agree on a protocol for the search process. Determine who will bear the costs of copying, searching, screening, and production. Use a screening procedure to protect non-responsive documents plus those protected by work product and/or attorney client privilege.[246]

IV. USING COMPUTER EXPERTS TO AID IN DISCOVERY AND TO ASSIST/SWAY COURT

A. Benefits of Retaining a Computer Forensics Expert

If a large amount of electronic information is significant to a given case, consider early retention of a computer forensics firm to assist in the collection, searching and production of that information.[247] Such a firm may help streamline the process and plan a strategy for discovery and production of electronic information. However, these experts can be costly. Therefore, you should assess your client's needs and resources when weighing the potential benefits against the anticipated significant costs. Moreover, as the quality of computer forensics firms varies greatly, you and your IT people should carefully scrutinize any such firm you – and thus your client – are contemplating retaining for the first time.

Expert testimony is also important if electronic discovery "meet and confer" negotiations reach an impasse. It is helpful in establishing or disproving whether the burdens of the requested discovery are outweighed by the benefits of obtaining information otherwise unavailable or in an inaccessible format. The lack of an expert may preclude

[245] *Id.*

[246] *See, e.g., Playboy Enters., Inc. v. Welles*, 60 F. Supp. 2d 1050, 1054-55 (S.D. Cal. 1999), *aff'd in part and rev'd in part on other grounds*, 279 F.3d 796 (9th Cir. 2002).

[247] Some of the more well-known forensic services providers are (in alphabetical order): Guidance Software <http://www.guidancesoftware.com/services/index.shtm>; KrollOntrack™ <http://www.krollontrack.com/eEvidence>; and New Technologies, Inc. ("NTI") <http://www.forensics-intl.com/>. Some of the many providers of collecting/searching/producing services are (in alphabetical order): Applied Discovery <http://www.applieddiscovery.com/>; Cataphora <http://www.cataphora.com/>; and Steelpoint <http://www.steelpoint.com>.

court enforcement of what might otherwise qualify as a valid discovery request.[248] Electronic discovery presents numerous complex logistical issues. It also entails intrusion into, and risks to the integrity and stability of, the target computer systems. If the parties must seek court intervention on such issues, they often will wish to educate the court on the technical issues via expert testimony. The requesting party must be prepared to demonstrate the basis for seeking the information; why it is expected to yield otherwise unavailable, discoverable information; and how the risks of harm and inconvenience can be minimized.

Experts can unearth a lode of significant electronic information from a range of sources, including companies' servers and individuals' hard drives. For example, late last year, the ability to uncover definitive electronic evidence loomed large in Plaintiff's voluntary dismissal, with prejudice, of a Massachusetts federal court case.[249] In that eviction dispute between two corporations, Plaintiff had attached to its Complaint hard copies of a purported lease addendum and of an allegedly accompanying transmittal e-mail. In a related lease action between the same parties, Defendant had "filed an ex parte motion to preserve . . . and expedite the production of electronic records[, alleg[ing] that both the . .. [a]ddendum and [transmittal] e-mail were fabricated by [Plaintiff]."[250] Accordingly, Defendant successfully contended "that it was necessary to allow [Defendant's] consultants to create mirror images of [Plaintiff's computer hard drives, back-up tapes and other data storage devices."[251]

Once Defendant's "consultants began mirror-imaging the electronic evidence," Plaintiff saw the writing on the wall (or, more accurately, on the hard drives). Realizing that the expert analysis would prove his fabrication, Plaintiff's President confessed. In the eviction action, Plaintiff's counsel then disclosed to the court and to opposing counsel that: the addendum had not existed when the parties signed the lease; and Plaintiff's President had "fabricated the [transmittal] e-mail by pasting most of a heading from an earlier, legitimate message and altering the subject matter line."[252] Plaintiff ultimately did not oppose Defendant's motion to dismiss, in effect agreeing to voluntarily dismiss the baseless lawsuit. Defendant was awarded almost $25,000, to cover expert costs and attorney fees.

In the web server context, consider the summary judgment opposition evidence submitted by Plaintiffs in the ongoing *Pharmatrak, Inc. Privacy Litigation*, 220 F. Supp. 2d 4

---

[248] *Goord*, 2002 U.S. Dist. LEXIS 8707, at *40-41.

[249] *Premier Homes and Land Corp. v. Cheswell, Inc.*, 240 F. Supp. 2d 97 (D. Mass. 2002) (awarding Defendant almost $25,000 in expert costs and attorney fees).

[250] *Premier*, 240 F. Supp. 2d at 98.

[251] *Id.* at 98.

[252] *Id.* at 98, 100.

(D. Mass. 2002).[253] *Pharmatrak* is a consolidated class action alleging various federal statutory violations by pharmaceutical sites and by *Pharmatrak*, a company those sites had hired to monitor and analyze web traffic. The gravamen of the claims is that Defendants used cookies and web bugs to engage in surreptitious accessing of browsing habits and confidential health information from the hard drives of visitors to those sites. Pursuant to court order, Plaintiff's expert, a computer scientist, examined *Pharmatrak'* servers.

According to the expert's subsequent declaration:

> Pharmatrak's logs "identified hundreds of people by name." . . . Pharmatrak [had] collected information which included: names. Addresses, telephone numbers, dates of birth, sex, insurance status, medical conditions, education levels, and occupations. Pharmatrak also collected data about e-mail communications, including user names, e-mail addresses, and subject lines from e-mails.[254]

In addition, based on that collected information, the expert was not only able to build user profiles but also to "assert[s] that it would be possible to build detailed profiles of individuals using the data collected by *Pharmatrak* and matching it to 'another data source, such as a telephone book.'"[255]

B. Relative Expertise of Opposing Experts

When deciding whether to compel electronic discovery, many a judge has come to expect an expert witness with sufficient computer expertise to provide a detailed explanation of the technical issues – such as how data might be obtained from a computer system and the likelihood that responsive information will be found.[256] Thus, the prevailing party in an electronic discovery dispute may very well be the one whose expert who has

---

[253] *Pharmatrak, Inc. Privacy Litigation*, 220 F. Supp. 2d 4 (D.Mass. 2002) (in seven consolidated class actions, dismissing Wiretap Act, Store Communications Act and Computer Fraud and Abuse Act claims), *reversed in part*, 2003 F.3d U.S. App. LEXIS 8598 (1st Cir. May 9, 2003) (reversing summary judgment grant as to Wiretap Act claim).

[254] *Pharmatrak*, 220 F. Supp. 2d at 9.

[255] *Id.* at 9.

[256] *New York State NOW v. Cuomo*, 1998 U.S. Dist. LEXIS 10520, *9. (where "no [Plaintiffs'] expert testimony describing in detail what would have been required," rejecting as speculative Plaintiffs' prejudicial delay contention - namely that delayed notice of destruction of database had precluded them from being able to enlist computer experts to un-delete the information); *Anti Monopoly*, 1995 U.S. Dist. LEXIS 16355, *8. (if parties are not able to resolve dispute about burden involved in compiling electronic data into report, they should submit follow-up motion, including affidavits from computer personnel or computer experts). *See also Fennell v. First Step Designs, Ltd.*, 83 F.3d 526 (1st Cir. 1996), also available at <http://laws.lp.findlaw.com/1st/952294.html> (rejecting request to copy Defendant's hard drive to determine creation date of allegedly back-dated termination memo because Plaintiff's computer expert could raise only possibility of achieving such determination).

better credentials and/or a more detailed explanation of his or her client's position.[257]

In a trade secret misappropriation dispute, the court focused on the opposing experts' relative credentials in assessing various sanction requests arising from Plaintiff's former employee's destruction of word processing files.[258] Plaintiff had hired a technician, whose credentials, experience, and knowledge were inferior to those of Defendants' retained expert, who had a Ph.D. in computer science from Stanford University. Consequently, the court placed far greater weight on Defendant's expert's testimony when assessing, and ultimately denying, Plaintiff's request for a default judgment.[259]

Additionally, Plaintiff's computer technician had bungled the copying of the pertinent hard drive, which he was to search for deleted files. The court had ordered Defendants to produce Plaintiff's former employee's computer to allow copying of the hard drive to obtain all available information regarding the deleted files. To compound Plaintiff's relatively weak position, its technician's attempt to recapture deleted, but not yet been overwritten, files had been ineffective.[260]

On the merits of Plaintiff's spoliation sanctions motion, Plaintiff's "challenge to the adequacy of the computer record . . . being provided" was justified by the former employee's destruction of computer files.[261] Yet, Plaintiff's expert's incompetence had ironically resulted in independent spoliation. Thus, the court awarded Plaintiff only ten percent of the fees and costs it incurred throughout the sanctions proceedings.[262]

---

[257] One case in which the relative merits of conflicting experts were dispositive was *Strasser v. Yalamanchi*, 669 So. 2d 1142 (Fla. 4th Ct. App. 1996), *review denied*, 805 So. 2d 810 (Fla. 2001). There, Plaintiff sought information previously purged from [D]efendant's computer system. Plaintiff submitted an affidavit of a CPA without any particular computer expertise. The CPA averred that it was "possible" to retrieve purged information. In contrast, Defendant's expert, a computer engineer, investigated the pertinent hardware and software, including the operation of the purging function. He examined the computer system for purged files, finding none. Weighing the competing experts' testimony, the court concluded that Plaintiff had failed to establish likelihood that the purged documents could be retrieved. *Id.* at 1145. *See also Alexander v. FBI*, 188 F.R.D. 111 (D.D.C. 1998).

[258] *Gates Rubber Co. v. Bando Chemical Indus.*, 167 F.R.D. 90, 110-11 (D. Colo. 1996), also available at <http://cyber.law.harvard.edu/digitaldiscovery/library/preservation/gates.html>.

[259] *Id.* at 111.

[260] Plaintiff's technician attempted to do the copying with an un-erase application. First, he unnecessarily made a copy of the pertinent program. Thus, even before commencing file-deletion, he overwrote seven to eight percent of the hard drive. The technician did not obtain the creation dates of some files that overwrote deleted files. That information would have helped determine some key deletion dates. As discussed in Section II(C) above, post-*Gate*s case law established a procedure whereby a neutral, third-party expert copies each relevant hard drive.

[261] *Id.* at 113.

[262] *Id.* Ironically, the failure to obtain the creation dates constituted spoliation that Defendants used to resist Plaintiff's spoliation allegations against Defendants.

V. CONCLUSION

As does its companion paper on efiling,[263] this paper raises more questions than it answers. Just how far must each side go to preserve evidence? How far may each go to hunt for evidence? Courts are grappling with these issues, though there are not yet clear-cut rules with broad applicability. Given today's burgeoning computer forensics capabilities, and the increasing volume of electronic data being generated,[264] the breadth of electronic discovery - and of the legal issues it implicates - can be overwhelming.

Reciprocity can act as a check on unreasonable and premature requests for intensive electronic discovery. When the parties are both businesses and/or the electronic discovery burdens weigh similarly on each side, there is an element of mutually assured destruction.

Be mindful that the law is constantly evolving and there are few absolute rules. But here are some suggestions to help keep your client in synch with electronic discovery rights and obligations:

(a) early on, inform the other side of the electronic information discovery you will be seeking and request that such information be preserved;

(b) promptly respond to a similar request from the other side, and inform it of any questions or objections;

(c) engage in a good faith dialogue with the other side, aiming to reach an early consensus about the desired scope of electronic discovery and the relevant expectations of each side;

(d) do not wait for a document request or a preservation letter or order; at the beginning of a dispute or case, start the process of searching for and collecting electronic information;

(e) ensure that your client and its employees are aware of the obligation to preserve evidence and the consequences of destruction, and advise them to communicate the attendant duties to the appropriate people;

(f) in responding to discovery requests and conducting searches, ensure your discovery efforts are above reproach; and

(g) choose your battles wisely; if you must seek the court's intervention, provide the court with all the information and explanation (including a well-credentialed expert) it will need to consider the salient issue(s).

---

[263] William A. Fenwick & Robert D. Brownstone, "Efiling," 19 SANTA CLARA COMPUTER & HIGH TECH L.J. 181 (2002), available at <http://www.fenwick.com>.

[264] As noted in footnote 2 *supra*: "The world produces between 1 and 2 exabytes of unique information per year, which is roughly 250 megabytes for every man, woman, and child on earth. An exabyte is a billion gigabytes, or 10^{18} bytes." Peter Lyman & Hal R. Varian, "*How Much Information*" (2000). <http://www.sims.berkeley.edu/research/projects/how-much-info/>.

The authors believe that, because of its volume, electronic information eventually will result in significant changes in discovery rules and procedures. Both the federal and state court systems are currently exploring the discovery implications of electronic information. At the federal level, the Discovery Subcommittee of the United States Advisory Committee on Civil Rules is assessing whether the of electronic information warrants proposed amendments to the Federal Rules of Civil Procedure. The Subcommittee's inquiry regarding the impact of computer-based materials is being coordinated by Special Consultant Richard L. Marcus, a Professor at UC Hastings College of Law.[265] In addition, at the state level, a National Center for State Courts (NCSC) project has been approved and funded. The Task Force for the NCSC project is being formed by the appointed project director Mary Durkin.[266]

[265] Richard L. Marcus, "*Is There a Need for Rule Changes to Address Distinctive Features of Discovery of Electronic Materials?*" (Sep. 2002).

[266] The National Center for State Courts (NCSC) <http://www.ncsconline.org/> has prepared a "not for publication" draft Project Proposal, "*Discovery of Electronic Evidence In State Court Civil Litigation*" (Dec. 2001).