January 2003

Ediscovery: Preserving, Requesting & Producing Electronic Information

Lisa M. Arent
Robert D. Brownstone
William A. Fenwick

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Part of the Law Commons

Recommended Citation
Available at: http://digitalcommons.law.scu.edu/chtlj/vol19/iss1/4

This Article is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
EDISCOVERY: PRESERVING, REQUESTING & PRODUCING ELECTRONIC INFORMATION

Lisa M. Arent†, Robert D. Brownstone†† and William A. Fenwick†††

† J.D. 1992, Indiana University School of Law, Bloomington, IN; B.A. 1989, University of Virginia. The author practices with the Litigation and Information Technology groups of Whyte Hirschboeck Dudek S.C. in Milwaukee, WI. The views expressed herein are those solely of the authors and cannot be attributed to the firm or its clients. For comments, the author may be reached at: lisaarent@yahoo.com.

†† Mr. Brownstone received his B.A. in English literature and political science in 1982 from Swarthmore College. He received his J.D. Magna Cum Laude in 1986 from Brooklyn Law School, where he was a Notes Editor and a published author on the Law Review. As Fenwick & West LLP’s Litigation Group knowledge manager and webmaster, Mr. Brownstone marshals the Group’s collective knowledge and develops technology tools to capitalize on that knowledge. Prior to joining Fenwick & West, Mr. Brownstone spent: six years as a full-time litigator in New York and San Francisco; and then eight years on a combination of ventures, as a litigator, consultant, law school administrator and law school adjunct professor. He is an active member of the California and New York bars, an inactive member of the District of Columbia and New Jersey bars and is also admitted to practice in many federal courts nationwide.

††† William A. Fenwick is one of the founding partners of Fenwick & West LLP and is a member of the firm’s Litigation and Intellectual Property Practice Groups. Mr. Fenwick received his B.S. in business management from Southern Illinois University where he graduated with Honors and was elected to Beta Gamma Sigma. He received his J.D. from Vanderbilt Law School and was elected to the Order of the Coif. Mr. Fenwick first began litigating technology disputes in 1968. Since 1992 he has been involved in a number of Internet-related matters as well as online commerce and communications. Since the early 1970’s, Mr. Fenwick has spoken and written extensively on privacy, on information handling and on the intersection of law and technology. He has served as Chairman, EFT Transfer Committee, American Federation of Information Processing Societies, Inc. and was one of the initial members of the Committee on Electronic Legal Research, New York Bar Association. Mr. Fenwick has served as Chairman, Committee on Law Relating to Computers, Section on Science & Technology. During his three years as Chairman of the Practicing Law Institute’s program on Computer Litigation, he was the editor of three volumes of working papers on various subjects related to law and technology.
I. INTRODUCTION

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.

The 1980 prediction was not too far off.

In our high-tech era, a body of law has evolved regarding the parameters of the preservation, collection, and production of electronic evidence. This Essay discusses the application 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 Essay, Professionalism in CyberDiscovery: The Proper Course for Retaining and Producing Electronic Documents, originally written and copyrighted in 1999 by Lisa M. Arent.


The world produces between $1 \text{ and } 2$ 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. 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.


3. An excellent and up-to-date compilation ("organized [both] by jurisdiction and by topic") of electronic discovery case blurbs is maintained by Kroll On Track at its Case Law List page. Kroll On Track, at http://www.krollontrack.com/LawLibrary/CaselawList (last visited Nov. 9, 2002). Other helpful resources include the "Library-Digital Discovery" list maintained by Harvard Law School and the "Electronic Discovery" case list maintained by CoreFacts. The Berkman Center for Internet & Society, Library - Digital Discovery, at http://cyber.law.harvard.edu/digitaldiscovery/library.html (last visited Dec 1, 2002); CoreFacts, Electronic Discovery, at http://www.corefacts.net/electronicdiscovery/electronicdiscovery_main.htm (last visited October 23, 2002).

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, BUS. J.
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 hard-copy documents, 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. 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. 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


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.


7. Rule 34 of the Federal Rules of Civil Procedure 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).” FED. R. CIV. P. 34(a). 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.”
modified Rule 34 to explicate that the term "documents" encompassed more than just hardcopies.\textsuperscript{8}

Neither of the California Discovery Act provisions regarding the production of "documents and tangible things" defines "document."\textsuperscript{9} Instead, in all Discovery Act sections, by virtue of section 2016(b)(3) of the California Code of Civil Procedure, "document" is coextensive with "writing" as defined in section 250 of the California Evidence Code. 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.\textsuperscript{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,\textsuperscript{11} and archival/emergency storage devices (such as back-up tapes).\textsuperscript{12} Moreover, electronic versions of documents can contain additional,

\textsuperscript{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." FED. R. CIV. P. 34(a). "[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 nondiscloseable matters, and costs." Id. See generally Hon. Shira A. Scheindlin & Jeffrey Rabkin, \textit{Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?} 41 B.C. L. REV. 327 (2000).

\textsuperscript{9} CAL. CIV. PROC. CODE. § 2031 (West 2001) (inspection and copying of documents and tangible things in possession, custody, or control of another party to the action); CAL. CIV. PROC. CODE. § 2020 (inspection and copying of nonparty's documents and tangible things).

\textsuperscript{10} Aguimatang v. California State Lottery, 234 Cal. App. 3d 769, 798 (1991) (computer's magnetic tapes constituted "writing" under section 250). See also MICHAEL R. OVERLY, OVERLY ON ELECTRONIC EVIDENCE IN CALIFORNIA § 3.05[A] (Robin Kojima et al. eds., 1999).

\textsuperscript{11} A "jaz drive" is "a removable disk drive" developed by Iomega Corporation. It "holds up to 2 gigabytes of data. The fast data rates and large storage capacity make it a viable alternative for backup storage as well as everyday use." Iomega, \textit{iomega Products}, at http://www.iomega.com/na/products (last visited Oct. 7, 2002).

non-printed information, such as the dates of creation, access and/or modification and, if relevant, sending and receiving details.  

2. Nature and Consequences of Duty to Preserve

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.

a. Ethical Obligations

When conducting discovery, an attorney should keep in mind several principles set forth in the 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.”

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[.]”

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). One category of potentially discoverable information beyond this Essay’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, 775 A. 2d 756 (N.J. App. Div. 2001) (upholding lower court ruling that corporation/defamation-plaintiff could not obtain identity of message-board-poster); Fenwick & West, Privacy & Information Security: Anonymity Online, at http://www.fenwick.com/About_Fenwick/Privacy_Law_Resources.htm#Anonymity (last modified Dec. 1, 2002) (listing other anonymity on-line decisions).

14. See also CAL. RULE OF PROF’L CONDUCT § 5-200(A) (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 PROF’L 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”); CAL. RULE OF PROF’L CONDUCT § 5-220.
b. 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 instructions, and even a dismissal or default judgment. The Second Circuit recently analyzed the requisite “culpable state of mind,” 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.”

c. 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.” To be 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 recently convicted on a federal obstruction/tampering
The criminal prosecution and a number of parallel civil lawsuits have been based on allegations that, while anticipating litigation, Andersen persuaded employees to shred Enron documents.

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. 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." 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 Andersen then embarked on an enormous spoliation effort.

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."

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

---


21. See, e.g., the Complaints in:


23. Id.

24. Id. (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.").

25. Id. at 6, para. 12.
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."\textsuperscript{26}

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, the answer, or discovery requests.

\textit{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 litigation.\textsuperscript{27} 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."\textsuperscript{28} 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.\textsuperscript{29} On the least culpable end of

\begin{itemize}
\item \textsuperscript{26} CAL. PENAL CODE § 135 (West 2002).
\item \textsuperscript{27} 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). \textit{See also} Mathias v. Jacobs, 197 F.R.D. 29, 39 (S.D.N.Y. 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)) \textit{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) ("[C]omplaint 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.").
\item \textsuperscript{29} 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. \textit{Id.} at 624–25 (citing, e.g., Wm. T. Thompson Co. v. Gen. 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).
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.” 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.

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 claims asserted.” That obligation arises before receipt of a production request.

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 Code of Civil Procedure, “[m]isuses of the discovery process [for which sanctions may be imposed] include, but are not limited to:

• “Failing to respond or to submit to an authorized method of discovery.”

• “Making an evasive response to discovery.”

30. Id. at 625.

31. See id. at 626 (concluding that the facts before it fit within the last category, namely alleged spoliation too remotely relevant to justify the imposition of tort liability). 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, 954 P.2d 511 (1998), the Supreme Court of California subsequently rejected Willard’s approval of the potential for tort liability for spoliation.


33. New York State NOW, 1998 U.S. Dist. LEXIS 10520 at *5 (“immaterial that the first document requests were not served until after the records were apparently destroyed”), Cedars-Sinai, 954 P.2d at 517 (destroying evidence in anticipation of discovery request would be misuse of discovery).
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." Generally speaking, a party should preserve those categories of evidence that it reasonably anticipates may later become relevant. 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, the defendant is obliged to preserve that division's sales correspondence and the like.

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." The most thorough communication would inform a...
client of the range of potential negative consequences of document and data destruction or deletion, including contempt of court, civil and criminal\textsuperscript{39} penalties, default judgment,\textsuperscript{40} or dismissal.

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, especially when mandated by a preservation order.\textsuperscript{41} Notice of the preservation obligation should be disseminated in a manner most likely to reach the employees—for example, in hard-copy form as well as by e-mail.\textsuperscript{42} 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 judgment, for a party’s failure to ensure that a preservation order is implemented and followed.\textsuperscript{43} Some cautionary tales emanate from three federal district court decisions. In a New Jersey federal class action, subsequent to defendant corporation’s feeble and

\textsuperscript{39} See, e.g., CAL. PENAL CODE § 135 (West 2002) (possibility of misdemeanor conviction for destruction of relevant evidence).

\textsuperscript{40} Teletron, 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).

\textsuperscript{41} 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”). 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. Prudential, 169 F.R.D. at 612. 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. \textit{Id.}

\textsuperscript{42} 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. Prudential, 169 F.R.D. at 613. Therefore, the use of e-mail communications was ineffective and failed to implement the court’s preservation order. \textit{Id.}

\textsuperscript{43} 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 a contempt finding, awarding reasonable attorney fees, expert fees and costs due to lack of compliance with order to preserve integrity of computers); \textit{Wm. T. Thompson Co.}, 593 F. Supp. at 1456 (striking GNC’s answer and dismissing GNC’s complaint in another action). \textit{Cf. Lang v. Hochman}, 92 Cal. Rptr. 2d 322 (Cal. Ct. App. 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).
deficient notification, four of the defendant’s field offices destroyed unauthorized sales materials as part of routine document destruction. The court chastised management for failing to take an active role in formulating, implementing, or communicating a document retention policy. Defendant’s “haphazard and uncoordinated approach to document retention indisputably denied the party opponent potential evidence to establish facts in dispute.”

Thus, the court drew the inference that the destroyed materials were relevant and, if available, would have led to successful proof of the claim.

In an earlier 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. 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.

Separate and apart from the litigation ramifications, corporate officers can be held personally responsible for a corporation’s 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. In that case, the CEO had delegated to the company’s “inexperienced” general counsel the entire responsibility for implementing a document preservation plan.

44. Prudential, 169 F.R.D. at 615.
45. 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.” Id.
46. Id.
47. Id.
49. 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.
51. Id.
Ediscovery: Electronic Information

In some cases, a party 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. "Plaintiffs have increasingly been demanding preservation of 'all' electronic data, including every single daily backup tape and file on a company system."\(^{52}\)

1. "Deleted" Files

"Deleted" does not necessarily mean gone forever. 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 contain "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.\(^{53}\) 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.\(^{54}\)

---

\(^{52}\) Electronic Evidence Discovery, Inc., A Balancing Act: Determining the Proper Level of Electronic Data Preservation, Recent Developments (June 1998), available at http://www.eedinc.com/staticcontent/resourceLibrary/RD%20June%2098.pdf. See also Hon. James M. Rosenbaum, In Defense of the Delete Key, 3 The Green Bag 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"). Note though, too an overly broad request can do more harm than good when one eventually appears before a judge on a discovery motion.


\(^{54}\) 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
a. Court-Ordered Hard Drive Searches

Does the obligation to search for and produce responsive computer data require a search for "deleted" files? 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.

At least three court decisions have granted requests for access to their opponents' computers. It is not entirely clear whether there overwriting some or all deleted files.

55. 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), available at http://www.abanet.org/litigation/taskforces/standards.html (last visited Dec. 2, 2002) (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").

56. 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); Gates Rubber Co. v. Bando Chem. 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); 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).


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), at http://www.fclr.org/2000fedctslrev2.htm (last visited Oct. 23, 2002). See also Fenwick & West, Order on Defendants' Motion for Protective Order & Plaintiffs Motion to Compel
was concrete evidence of data destruction in two of those cases. In contrast, the third case did involve actual data destruction. In any event, taken together, these three cases arguably represent a trend in federal courts to appoint neutral experts to copy hard drives and 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. In one such case, the neutral expert confirmed that plaintiff had submitted an altered e-mail in opposition to a motion. The court dismissed the complaint, ordering the 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."

In a more recent 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. The claims arose from an allegedly wrongful termination based on the

---


Note, though, that at least one commentator has questioned the neutrality of the Northwest Airlines expert. Sandra Rosenzweig, Rosie's Ramblings, CAL. LAW. (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.").


59. 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).

60. See Munshani v. Signal Lake Venture Fund II, 2001 Mass. Super. LEXIS 496, *3–4 (Oct. 9, 2001), 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.

61. Id. at *5.

62. Id. at *7.

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 California Constitution article 1 section 1, "the employee had no reasonable expectation of privacy when he used the home computer for personal matters, the appellate court directed the trial court to order the requested discovery." 64

b. 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. 65 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. 66 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

---

64. Id. Though a potential federal e-mail monitoring claim by an employee is beyond the scope of this Essay, note that the Electronic Communications Privacy Act ("ECPA") 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." 18 U.S.C. § 2511(2)(h)(ii) (2002).

65. Lexis-Nexis v. Beer, 41 F. Supp. 2d 950 (D. Minn. 1999). As he was leaving his employment with LexisNexis, 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 LexisNexis 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.

66. 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.
the employee for his discovery abuses and his clear violation of both parts of the discovery order.\textsuperscript{67}

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, the Northern District of California sanctioned a defendant for its egregious removal of website information in an attempt to avoid California personal jurisdiction.\textsuperscript{68} In opposing a jurisdictional motion to dismiss, the plaintiff alleged that the defendant company had maintained a California office. The plaintiff submitted a printout of a page from the defendant's website that had displayed that office's contact information. The web page subsequently "disappeared" shortly after the filing of the motion. The defendant initially denied that the web page "ever existed on its web site or on any location authorized by Defendant."\textsuperscript{69} Then, "[i]n a sudden resurgence of memory," the defendant recalled deleting the page "as part of 'routine maintenance,' but provided no details whatsoever about this alleged practice."\textsuperscript{70} When faced with this obvious duplicity, the court sanctioned the 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.\textsuperscript{71} Because the defendant eventually stipulated to jurisdiction, an order establishing personal jurisdiction pursuant to Rule 37(b)(2), while justified, was not necessary.\textsuperscript{72}

\textsuperscript{67} \textit{Lexis-Nexis}, 41 F. Supp. 2d at 955. The court, however, declined to draw any adverse evidentiary inferences. \textit{Id.} at 954--55. The court was not convinced that LexisNexis could show that evidence pertinent to the litigation was actually destroyed. \textit{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. \textit{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. \textit{Id.} at 955 (relying on Gates Rubber Co. v. Bando Chem. Indus., 167 F.R.D. 90, 104 (D. Colo. 1996)).


\textsuperscript{69} \textit{Id.} at *5.

\textsuperscript{70} \textit{Id.} at *6.

\textsuperscript{71} \textit{Id.} at *14.

\textsuperscript{72} \textit{Id.}
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. 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 tens of thousands of dollars. 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 excessively duplicative and irrelevant data."

   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

75. Id. at 262.
date, coinciding with the date on which the preservation effort is made, then additional back-up tapes from later dates would not be important.\textsuperscript{76} 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—\textit{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.

\textit{b. Failure to Cease Ordinary Recycling}

Some courts have enforced preservation obligations regarding back-up tapes. For example, in one case, \textit{Linnen v. A. H. Robins Company},\textsuperscript{77} the plaintiff succeeded on a sanctions motion, based on a theory that the defendant's failure to preserve back-up tapes during the first four months of the lawsuit was tantamount to evidence destruction.\textsuperscript{78} The 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 the plaintiff, the challenged four-month period was critical to the underlying product liability claim, in that it had immediately preceded the defendant's decision to remove from the market the relevant pharmaceutical product.

\textsuperscript{76} 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.

\textsuperscript{77} \textit{Linnen}, 1999 Mass. Super. LEXIS at 240 (June 16, 1999).

\textsuperscript{78} \textit{Id.} 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). \textit{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.
In light of an *ex parte* preservation order (albeit temporary) and the service of production requests, the defendant was obliged to preserve the back-up tapes.\(^7^9\) Because the defendant did not fulfill that obligation, the court granted spoliation sanctions, including a jury instruction permitting the inference that the defendant had destroyed potentially relevant evidence out of a realization that the evidence was unfavorable.\(^8^0\)

Similarly, another court imposed spoliation sanctions for a party’s failure to preserve back-up tapes that were the only source of relevant information.\(^8^1\) The 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.\(^8^2\) Once served with a document request, the defendant 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.”\(^8^3\) The court rejected’s putative excuse that the plaintiff had been previously informed of the routine deletion of back-up files but had not asked the defendant to save them.\(^8^4\) The defendant had an independent, “affirmative” preservation duty.\(^8^5\)

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

---

79. In particular, the court ruled that:

During the period of time when the *ex parte* order requiring defendant 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 made it clear that plaintiffs sought the production of items such as the system back-up tapes and, after receiving this request, defendant had an obligation to preserve any such documents or materials.

*Id.* at *29–30* (emphasis added).

80. *Id.* at *37.


82. *Id.* at *11.

83. *Id.*

84. *Id.*

85. *Id.*
Courts are now unlikely to be swayed by a high tech company that balks at the prospect of back-up restoration. For example, in Linnen, the court did not look kindly on the lead defendant’s stonewalling. Robins had produced only a small number of e-mail messages, in hard-copy 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, the 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.

The 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, the 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 “had the potential for containing relevant material and that the plaintiffs should have the opportunity to examine at least a portion . . . to determine if that is the case.”

The defendant argued that restoring and searching back-up tapes would be an unduly burdensome “multi-million dollar fishing expedition.” The court disagreed, noting that the plaintiffs had tailored the request to seek specific responsive e-mails. The court

---

86. 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.”). 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).


88. Id. at *16.

89. Id. at *17.

90. 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
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 the defendant would produce to the plaintiffs. Then, the plaintiffs could revisit their request for production.91

In a more recent decision, McPeek v. Ashcroft, 92 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.93

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 which the 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. Part of the cost at hand stemmed from 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." As a
result, the court only ordered the DOJ to perform a backup restoration
of the e-mails to and from the plaintiff's supervisor for a one-year
period.

Even more recently, a Second Circuit jury verdict reversal
reinforced the judicial trend of scrutinizing companies' contentions
that they cannot recover data stored on back-up tapes. In Residential
Funding Corporation v. DeGeorge Financial Corporation, the
appellate court found that the trial court had not adequately dissected
the 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 the defendant's consultant's ability, to
recover 950,000 e-mails from the pertinent time period in four days.

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. 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.\textsuperscript{100}

This requirement was illustrated in Fennell v. First Step Designs, Ltd.,\textsuperscript{101} a discrimination case, in which a discharged employee sought creation-date evidence for a memorandum regarding some layoffs, including her own. The defendant produced a copy of the memo on computer disk. When the plaintiff could not determine the creation date, she sought access to the 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 [the plaintiff] would have access to relevant materials."\textsuperscript{102} The defendant objected to the plaintiff's proposed protocol, which entailed a technician copying the entire hard drive, analyzing the copy off site, and later erasing the copy.\textsuperscript{103} The defendant submitted its own detailed protocol, which the court described as "extremely cumbersome and expensive."\textsuperscript{104}

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.\textsuperscript{105} It concluded that the hard drive copying presented a low likelihood of success, along with substantial risks and costs.\textsuperscript{106} The First Circuit affirmed, noting that the lack of detail in the plaintiff's protocol "cast even more doubt on the soundness of the technical basis for the discovery venture."\textsuperscript{107}


\textsuperscript{101} Fennell, 83 F.3d at 526.

\textsuperscript{102} 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).

\textsuperscript{103} 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.

\textsuperscript{104} Id.

\textsuperscript{105} Id.

\textsuperscript{106} Id.

\textsuperscript{107} Id. at 533.
Similarly, a state court of appeal reversed an order that had given the plaintiff unlimited access to the defendant's computer system in *Strasser v. Yalamanchi*. In *Strasser*, the plaintiff/docotor sought to inspect the computer system of the defendant, his ex-colleague. The plaintiff desired to locate and recover previously purged financial data. The defendant objected, claiming that the search would "allow carte blanche access, unlimited in scope, nature or purpose." Ultimately, the trial court ordered the requested discovery. On appeal, though, the court agreed with the defendant that unfettered access was inapt, especially given the lack of any solid evidence of data recoverability. Moreover, even if there had been recoverability evidence, a tailored search would have been justified only if no other less intrusive means existed.

In each of the three relatively recent decisions mentioned in section II(B)(1)(b) above, a court has appointed a neutral computer expert to copy the defendant’s to-be-searched computer hard drive to try to recover deleted files. Each court required that the requesting party, the plaintiff, would pay the expert’s resultant fees and costs. 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 turned over to defense counsel for pre-production review for privilege and responsiveness.

---


109. *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.

110. *Id.*

111. *Id.* at 1145. 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 defendant's computer and databases."


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 hard-copy form does not preclude the requesting party from receiving that same information in computerized form.\textsuperscript{115} A court may also require a party to compile electronic data into a particular format or structure requested by the opposing party.\textsuperscript{116} If a request is burdensome, a court may require the requesting party not only show the need for the information but also agree to pay the costs of production.\textsuperscript{117} If the respective merits of the justification-versus-burden analysis are uncertain, the court may order the parties to the negotiating table.\textsuperscript{118}

2. Compelling Creation of Electronic Information

In a very recent 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.\textsuperscript{119} The suit was brought by television executives and movie studios (extending confidential information access to two in-house attorneys for each Defendant, contingent on their compliance with protective order).

\begin{itemize}

\item \textsuperscript{116} Anti-Monopoly, 1995 U.S. Dist. LEXIS 16355, at *1 ('the 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.'). \textit{See also} Nat'1 Union Elec. Corp. v. Matsushita Elec. Indus. Co., 494 F. Supp. 1257, 1258-59 (E.D. Pa. 1980) (requiring plaintiff in antitrust case 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). \textit{But see Replay} decision discussed in section II(D)(2).

\item \textsuperscript{117} Anti-Monopoly, 1995 U.S. Dist. LEXIS 16355, at *3.

\item \textsuperscript{118} \textit{See id.} 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. \textit{Id.}

\end{itemize}
regarding the Replay TV 400, a personal video recorder (PVR) that enables users to, among other things, store television programs for later viewing and skip commercials.

The plaintiffs had sought discovery of documents and information regarding the defendants’ customers, including identification of the television shows that the customers had recorded. In support of their request, The plaintiffs contended that “there [was] nothing unusual about directing a party to create software to ‘retrieve information stored in computers.’” They argued that there is “a duty to extract relevant information to respond to an interrogatory.”

Initially, the magistrate judge ordered the requested discovery. The defendants obtained a stay of the magistrate’s order upon filing a motion for district judge review of the order compelling discovery. In their motion for review, the defendants emphasized that the requested items were never in their possession because they have opted not to monitor customer usage. 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


121. Id. 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. Department 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’); and Henderson v. National R.R. Passenger Corporation, 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).


units to Defendants' servers, to be stored indefinitely, and made available to Plaintiffs in the litigation.\textsuperscript{125}

The 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 [their] servers."\textsuperscript{126} The defendants asked the court to distinguish prior compilation production cases\textsuperscript{127} as having entailed either retrieval or software design to enable the extraction of already extant electronic business records.\textsuperscript{128} They posited that, in contrast, a party cannot be "required 'to prepare, or cause to be prepared,' new documents solely for their production."\textsuperscript{129}

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."\textsuperscript{130} The district court judge accepted the defendants' interpretation of Rule 34, ruling that "the information sought by plaintiffs is not now and has never been in existence. The [portion of the Magistrate's] Order requiring its production is therefore contrary to law."\textsuperscript{131} 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 hard-copy production. For example, in an

\begin{itemize}
\item \textsuperscript{125} Id. at 2.
\item \textsuperscript{126} Id.
\item \textsuperscript{128} Review Brief, supra note 124, at 7, n.7, 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.
\item \textsuperscript{129} Alexander v. FBI, 194 F.R.D. 305, 310 (D.D.C. 2000).
\item \textsuperscript{130} Review Brief, supra note 124, at 8.
\item \textsuperscript{131} Id. at 2.
\end{itemize}
employment discrimination case, the Seventh Circuit upheld the trial court's decision to deny the plaintiff's motion to compel production of what would have amounted to 210,000 hard-copy pages of e-mails. The defendant had initially produced the e-mails on four-inch tapes, an inaccessible format for the 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 necessary software, or offer him on-site access to its own system. Only if those options ultimately failed (and they did not in this case) would the court have ordered the parties to split the cost of copying the e-mails in hard-copy form.

In a very recent decision, practical considerations seemed to hamstring a judge who might otherwise have required the defendant to produce "data in electronic, manipulable form [to] facilitate expert analysis." Goord is 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:

[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

133. Id. at 1171. Cf. GTFM, Inc. v. Wal-Mart Stores, 2000 U.S. Dist. LEXIS 3804 (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).
134. Sattar, 138 F.3d at 1171.
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.\footnote{136}

Four practical considerations doomed the plaintiff’s “plausible claim” that “manipulable data” was needed.\footnote{137} First, even though he acknowledged the financial constraints of pro bono counsel, the judge was troubled by the plaintiffs’ lack of an expert, as this deficiency rendered the plaintiffs’ discovery plan quite general.\footnote{138} Second, much of what the inmates hoped to discover was contained in more than 700,000 pages of hard-copy records already produced in paper form, at considerable state expense.\footnote{139} Third, the factual context entailed the same type of “significant security[/confidentiality] concerns” typically found in trade secrets cases “in a business context.”\footnote{140}

Lastly, the 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.\footnote{141} Therefore, the court declined to “impose additional burden, expense and risk of harm on the parties, and especially on the defendants, at this belated hour, after the expenditure of so much effort and expense, and on the undocumented hope of obtaining such speculative benefits.”\footnote{142}

In contrast, in another civil case against the government, a state’s highest court went quite far in finding the discoverability of electronic

\footnotesize{136. Id. at *28–29, *31.  
137. 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?  
138. 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, at *1–2 (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 hard-copy had been altered. The court found that plaintiff’s request “was supported by nothing more than speculation that defendant had somehow altered its e-mails before producing them.”  
140. Id. at *37.  
141. Id. at *46–47.  
142. Id. at *48.}
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 similar consolidated case.

Of potential significance for future electronic discovery disputes was the court's observation that:

> As governments everywhere move from paper and microfiche 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.

### 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. 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. In balancing such factors in various factual contexts, federal district court cases have reached disparate outcomes.

Some decisions have shifted to the requesting party the costs of compiling and producing electronic information. In the *Linnen...*
fen/phen class action, the court ordered the responding party to bear the expenses of back-up tape restoration. Yet, the 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.

Other decisions have declined to remove the cost burden from the shoulders of the responding party. In one such instance, a court mandated payment of all expenses unnecessarily incurred because of the defendant's inaccurate disclosure of its computer capabilities.

In another case, a federal antitrust class action, the plaintiffs sought to compel one of the defendants, Ciba-Geigy Corp. ("Ciba"), to produce responsive, computer-stored e-mails at its own expense. Ciba objected, arguing that the request was overly broad and burdensome, and that the plaintiffs should bear the retrieval costs. Ciba estimated that 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.


149. 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).

150. 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.


154. _id. at *1.
The court declined to impose on the plaintiffs that cost because it resulted from Ciba's record-keeping scheme and its choice of electronic storage. The court only required the 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.

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.

155. Id. at *2.
156. Id. at *8.
157. 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
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. 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. The absence of a court order may narrow the scope of the available sanctions should evidence destruction ensue.

In one case the defendant moved for sanctions based on plaintiff Procter & Gamble’s (P&G) alleged destruction of e-mail material could be extracted), aff’d & rev’d on other grounds, 222 F.3d 1262 (10th Cir. 2000).

158. 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 (1991)).

159. 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), 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, (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”),

160. 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), aff’d in part & rev’d in part on other grounds, 222 F.3d 1262 (10th Cir. 2000).
communications. In the absence of a preservation 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. The 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 the plaintiff's searches, with the exception of the deletions of the e-mail of five individuals whom the plaintiff itself had identified as having relevant information. 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.

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." 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]."

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.

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

162. Id.
163. Id. at 631.
165. Id.
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 emails, spreadsheets and databases relating to specified topics, then specify those items in the requests themselves. 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 defendants’ computer system or to canvass all of the defendants’ debtor files.”

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 recent case, DeLoach v. Philip Morris Companies, the defendants claimed that the discovery request for “all summary documents” (including electronic data) was overbroad. The plaintiffs alleged that the 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 [d]efendants until after [defendants’] rebuttal report was submitted, after [p]laintiff's expert report had been submitted and [p]laintiffs’ expert had been deposed.”

The court

167. 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., 89 Cal. Rptr. 2d 353 (1999) (“definition of ‘document’ in deposition notice included computer tapes, discs and any information stored in a computer”).

168. 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.


171. 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. Philip Morris, 206 F.R.D at 573. “[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.

172. Id. at 573. Defendant then deleted more than two million entries (without informing
found that the defendant "should have produced the disputed database." 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."

In a dispute between competing software companies regarding allegedly improper copying and use of proprietary source code, the plaintiff sought production of the entire source code for each of the defendant's products from the previous three and one-half years. The plaintiff also requested copies of all hard drives that had access to the server from which the information at issue was purportedly copied. The court ruled that "production 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."

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 Federal Rule of Civil Procedure 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 recently pointed out:

In the electronic age, this [Rule 26(f)] meet and confer should include a discussion of 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.

plaintiff of the deletion) and provided plaintiff with "the single item that was specifically and unambiguously requested." Id.
173. Id. at 574.
174. Id.
176. Id.
177. Id.
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, hard-copy 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.179

("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 into electronic form in favor of requiring plaintiffs "to pay the nominal cost of duplicating compact discs."). See also CAL. CIV. PROC. CODE §§ 2017(c)-(d), 2025(g), (o), 2031(f), (m), 2033(e), (l) (West 2002) ("[G]ood faith attempt at an informal resolution" required by, among other provisions); CAL. CIV. PROC. CODE § 2017(e) (West 2002), ("[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), Meet and Confer, CALIFORNIA DISCOVERY (1999), at http://californiadiscovery.findlaw.com/MEET_AND_CONFER_WEB.htm (last visited Oct. 22, 2002).

179. A discovery issue beyond the scope of this Essay is the ability to take depositions over the Internet. The Federal Rules of Civil Procedure ("FRCP") expressly provide 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." FED. R. CIV. P. 30(b)(7); See also Vt. R. CIV. P. 30(b)(7). "Increasingly, parties are conducting depositions by remote electronic means due to 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, CALIFORNIA DISCOVERY, at http://californiadiscovery.findlaw.com/Internet_Discovery.htm (last visited Oct. 22, 2002) (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.").


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

**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 Director. In federal court Rule 30(b)(6) depositions can be used to avoid using up many of the allowed depositions.

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.

---

181. *Id.* at *13–14. See also Jones v. Goord, 2002 U.S. Dist. LEXIS 8707, at *48 (denying electronic discovery request deemed "belated" and "speculative" due to six year delay and lack of a specific—let alone expert-based—discovery plan).
182. 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. FED. R. CIV. P. 30(b)(6). Thus, 30(b)(6) depositions are outside the scope of the "leave of court" a party must obtain to exceed the ten deposition limit set by FRCP Rule 30(a)(2)(A), and Rule 31(d)(2)(A) ("Deposition Upon Written Questions").
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,\(^\text{184}\) 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.\(^\text{185}\)

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 the plaintiffs resulting from the defendants’ failure to produce information from a database was mitigated by the plaintiffs’ ability to obtain that information from a third party.\(^\text{186}\) And another court denied an emergency \textit{ex parte} application for a temporary restraining order to prevent anticipated destruction and concealment of computer files, ruling that “[p]laintiffs’ own complaint and... application reveal[ ] ample alternative sources of proof.”\(^\text{187}\)

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

---


\(^{185}\) Third party services are sometimes used 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.


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.  

If a defendant proves uncooperative in discovery, a court may be more receptive to a plaintiff’s request for extensive electronic discovery. For instance, in Tulip v. Dell Computer Corporation, a patent case, the court granted the plaintiff’s customized discovery request that the defendant make its senior executives’ e-mail records available, after having an opportunity to address privilege and confidentiality concerns. The plaintiff’s proposed procedure was deemed “fair, efficient, and reasonable.” The 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.” The plaintiff was directed to give the defendant a list of e-mails containing those terms, but was not to read the e-mails until the defendant had an

188. 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. 2002) (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).


190. 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.

191. Id.

192. Id.
opportunity to review them to ensure that privilege and confidentiality concerns were not compromised.\textsuperscript{193}

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.\textsuperscript{194} To support their various claims, the plaintiffs sought to discover “the names and addresses of passengers included in [one of four] computer database[s] ... provided during [previous] discovery.”\textsuperscript{195} The 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.”\textsuperscript{196} Plaintiffs also sought to contact a sampling of nonparty passengers to interview them about their Customs treatment. The court ordered the 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.”\textsuperscript{197}

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

\textsuperscript{193} Id.
\textsuperscript{195} Id. at *9.
\textsuperscript{196} Id. at *16.
\textsuperscript{197} Id. at *24–25.
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.

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 supra 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.

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 the plaintiff for failing to search or preserve the e-mail communications of five key employees whom the plaintiff had identified as having relevant information. 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 on whether they 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.

198. *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").
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. Store originals in a secure place—i.e., a place of limited and controlled access—to avoid the possibility of data corruption via alteration or destruction. 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:

---

200. Id.
• 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.\(^{201}\)

IV. USING COMPUTER EXPERTS TO AID IN DISCOVERY AND TO ASSIST/SWAY THE 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 searching, collection, and production of that information. 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.

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 court enforcement of what might otherwise qualify as a valid discovery request.\(^{202}\) 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

\(^{201}\) See, e.g., Playboy, 60 F. Supp. 2d 1050, 1054–55.

seeking the information; why it is expected to yield otherwise unavailable, discoverable information; and how the risks of harm and inconvenience can be minimized.

B. Relative Expertise of Opposing Experts

An expert witness with sufficient computer expertise should provide a detailed explanation of the technical issues, such as how data might be obtained from the computer system and the likelihood that responsive information will be found. The prevailing party in an electronic discovery dispute may be the one whose expert has better credentials and/or a more detailed explanation of his or her client’s position.

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

203. New York State NOW v. Cuomo, 1998 U.S. Dist. LEXIS 10520, *9 (where “no [plaintiff’s] 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, at *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, (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).

204. One case in which the relative merits of conflicting experts were dispositive was Strasser v. Yalamanchi, 669 So.2d 1142, rev. 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, 188 F.R.D. at 111.


206. Id. at 111.
Additionally, the plaintiff’s computer technician had bungled the copying of the pertinent hard drive, which he was using to search for deleted files. The court had ordered the defendants to produce the plaintiff’s former employee’s computer to allow copying of the hard drive to obtain all available information regarding the deleted files. To compound the plaintiff’s relatively weak position, its technician’s attempt to recapture deleted, but not yet been overwritten, files had been ineffective.  

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.  Yet, the plaintiff’s expert’s incompetence had ironically resulted in independent spoliation. Thus, the court awarded only ten percent of the fees and costs it incurred throughout the sanctions proceedings.  

V. CONCLUSION

As does its companion Essay on eFiling, this Essay 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, 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 in litigation, 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).

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 nature 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.\textsuperscript{211} 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.\textsuperscript{212}

\begin{flushright}
\begin{minipage}{\textwidth}
\footnotesize
\bibitem{211}Richard L. Marcus, \textit{Is There a Need for Rule Changes to Address Distinctive Features of Discovery of Electronic Materials?}, National Center for State Courts (Sept. 2002)
\bibitem{212}National Center for State Courts, \textit{Discovery of Electronic Evidence In State Court Civil Litigation}, (Dec. 2001). This draft project proposal is “not for publication.” (on file with author).
\end{minipage}
\end{flushright}