2000

E-discovery: Preparing Clients for (and Protecting Them Against) Discovery in the Electronic Information Age

Carey Sirota Meyer

Kari L. Wraspir

Follow this and additional works at: http://open.mitchellhamline.edu/wmlr

Recommended Citation


This Article is brought to you for free and open access by the Law Reviews and Journals at Mitchell Hamline Open Access. It has been accepted for inclusion in William Mitchell Law Review by an authorized administrator of Mitchell Hamline Open Access. For more information, please contact sean.felhofer@mitchellhamline.edu. © Mitchell Hamline School of Law
E-DISCOVERY: PREPARING CLIENTS FOR (AND PROTECTING THEM AGAINST) DISCOVERY IN THE ELECTRONIC INFORMATION AGE

Carey Sirota Meyer†
Kari L. Wraspir‡†

I. INTRODUCTION ......................................................................................... 940

II. LEGAL IMPLICATIONS: COURTS ARE EMBRACING THE NOTION OF E-DISCOVERY ................................................................. 941
   A. The Approval of Electronic Discovery Under the Rules of Civil Procedure and Judicial Decisions .............................................................. 941
   B. The Extent of Discovery Permitted .................................................. 943
      1. Types of Discoverable E-Data .................................................. 945
         a. Active Data or Data Files .................................................. 945
         b. Replicant Data .......................................................... 946
         c. Residual Data .......................................................... 948
         d. E-Mail ................................................................. 949
      2. Limitations of E-Discovery .................................................... 951
         a. Overbroad and Unduly Burdensome Objection Successful .......................................................... 951
         b. Cost as Basis for Objection ........................................ 952
         c. Attorney-Client Privilege and Work Product Objections Still Apply .................................................. 953

III. PRACTICAL APPLICATIONS: GETTING CLIENTS IN THE BEST

† Carey Sirota Meyer is an associate in the Minneapolis office of Oppenheimer Wolff & Donnelly LLP, practicing in the area of business litigation. Ms. Meyer received her Bachelor of Arts degree, cum laude, from the University of St. Thomas. She received her Juris Doctor degree, magna cum laude, from William Mitchell College of Law, where she was an Associate Editor of the William Mitchell Law Review. The views expressed in this article should not be attributed to Oppenheimer Wolff & Donnelly LLP, or any of its clients.

‡† Kari L. Wraspir is an associate in the Minneapolis office of Oppenheimer Wolff & Donnelly LLP, practicing in the area of business litigation. Ms. Wraspir received her Bachelor of Arts degree, magna cum laude, from Gustavus Adolphus College and her Juris Doctor degree, summa cum laude, from William Mitchell College of Law, where she served as an Editor of the William Mitchell Law Review. The views expressed in this article should not be attributed to Oppenheimer Wolff & Donnelly LLP, or any of its clients.
I. INTRODUCTION

Computers, e-mail, e-commerce, and the Internet dominate and are changing the landscape of the business marketplace. These once unimaginable innovations have undoubtedly simplified business—in most cases, anyway. From a legal standpoint, the injection of technology into the business world has actually complicated matters. One type of technology can be especially burdensome—electronic mail or e-mail. With e-mail often replacing a formal letter or voicemail, the type and volume of business communications have increased dramatically. This proliferation is proving to be a source of liability for some companies due to improper use of e-mail by employees. More importantly, the accumulation of massive amounts of e-mail can unnecessarily increase the time and expense involved in litigation discovery. In addition, with individuals tending to communicate candidly in e-mail, overzealous attorneys go to great lengths to obtain e-mail, as this new medium may contain the "smoking gun" in litigation. With technology changing the face of business and presenting new challenges in litigation, attorneys and their clients are left with the daunting task of understanding how to prepare for and tackle "e-discovery." 1

1. By "e-discovery," the authors mean discovery of data and information in electronic form. The breadth of data encompassed by this term is addressed in...
The purpose of this article is to familiarize corporate and defense attorneys with the issues presented by e-discovery and to provide suggestions as to how to tackle it in litigation. This article will first address the courts allowance of e-discovery, the extent to which electronic information and data are discoverable, and potential limitations to discovery. Second, the article will practically apply judicial trends by outlining how attorneys can assist their clients to be in the best possible position to deal with e-discovery and the issues of the technology age. In doing so, this article provides suggestions for e-mail and Internet usage policies to better control volume and content of electronic data, and offers steps a business can implement to make the organization and storage of electronic information more manageable and discovery-friendly. Third, the article outlines what constitutes a good faith reasonable search for purposes of responding to discovery requests. Finally, the article provides anecdotal examples of the hazards of electronic information in the litigation context.

II. LEGAL IMPLICATIONS: COURTS ARE EMBRACING THE NOTION OF E-DISCOVERY

A. The Approval of Electronic Discovery Under the Rules of Civil Procedure and Judicial Decisions

Federal Rule of Civil Procedure 34, and its Minnesota counterpart, provide for the discovery of documents and other information from opposing parties. Historically, “documents” has meant tangible paper documents. As society and the business world have changed with technology, the landscape for and the scope of discovery in litigation has transformed as well.

The Federal Rules of Civil Procedure and courts have also adjusted to the change. The text of Rule 34 provides for e-discovery by permitting the discovery of any “data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably useful form.” The Advisory Committee Notes to Federal Rule of Civil Procedure 34 further provide that:

greater detail below. See infra Part II.B.1.

2. See MINN. R. CIV. P. 34.01.

3. FED. R. CIV. P. 34(a). The text of Rule 34 was amended in 1970 to add this “data compilation” language. See id. (1970 advisory comm. note).
The inclusive description of "documents" is revised to accord with changing technology. It makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when 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. In many instances, this means that respondent will have to supply a printout of computer data. The burden thus placed on respondent will vary from case to case, and the courts 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. Similarly, if the discovering party needs to check the electronic source itself, the court may protect respondent with respect to preservation of his records, confidentiality of nondiscernable matters, and costs.4

The Manual for Complex Litigation also contemplates addressing the process for discovering electronic data in litigation discovery schedules.5 Specifically, the Manual for Complex Litigation advises that "[a]ny discovery plan must address relevant issues, such as the search for, location, retrieval, form of production and inspection, preservation, and use at trial of information stored in mainframe or personal computers or accessible 'online.'"6

Courts have followed suit noting that "it is black letter law that computerized data is discoverable if relevant."7 Another court has noted that "[c]omputers have become so commonplace that most court battles now involve discovery of some type of computer-stored information."8 Citing its state equivalent to the federal discovery rules, a recent Massachusetts superior court decision noted:

[a] discovery request aimed at the production of records retained in some electronic form is no different, in principle, from a request for documents contained in an office file cabinet. While the reality of the situation may require a different approach and more sophisticated equipment than a photocopier, there is nothing about the technological aspects involved, which renders documents stored in an electronic media "undiscoverable." 9

That being the current judicial sentiment, 10 counsel must understand the breadth of available discovery to prepare to litigate on this new battleground.

B. The Extent of Discovery Permitted

Like any other business record, electronic media 11 is discoverable in litigation and may be used as evidence in a


10. With the potential costs of e-discovery and its attendant burdens on litigants, see infra Part II.B.2, the present discovery framework may not suffice to adequately manage these issues. In fact, the Federal Civil Rules Advisory Committee has recently decided to proceed with a study of e-discovery. As the law develops as courts and the Federal Civil Rules Advisory Committee address these issues, separate discovery rules may emerge. Until then, counsel and their clients must proceed under the current framework.

11. Electronic media includes the following:

Data files which can be found on (1) office desktop computers and workstations; (2) notebook computers; (3) home computers; (4) computers of personal assistants/secretaries and staff; (5) palmtop/handheld devices; and (6) network file servers and mainframes.

Back-up tapes including (1) system-wide back-ups (monthly, weekly or incremental); (2) disaster recovery back-ups which are stored offsite; and (3) personal or "ad hoc" back-ups which can be on diskettes and other portable media.

Other media sources such as: (1) tape archives; (2) replaced or removed drives; and (3) floppy diskettes, CDs, Zip disks or other portable media.

Joan E. Feldman & Rodger I. Kohn, The Essentials of Computer Discovery, 564 PLI/PAT 51, 57 (1999); see also MANUAL FOR COMPLEX LITIGATION § 21.446 (noting that computerized data includes "operating systems (programs that control a computer's basic functions), applications (programs used directly by the operator, such as word processing or spreadsheet programs), computer generated models, and other sets of instructions residing in computer memory"); infra Part II.B.1.
courtroom. As with all other discovery, computer or electronic data is discoverable if the request satisfies the requirements of Rule 26. In other words, the information must be relevant to the subject matter of the lawsuit, not unnecessarily cumulative or duplicative; the burden or expense must not outweigh its benefit; and it must not be subject to a claim of privilege nor protected by the work product doctrine. Given that the "relevance" threshold is low—"reasonably calculated to lead to the discovery of admissible evidence"—attorneys focus on these standard objections to curtail and limit e-discovery, as it is often more expensive and time consuming to produce than its paper counterpart. The most fertile ground for thwarting such discovery is the undue burden and expense objection. While courts have been quite generous in permitting broad discovery of electronic data, however, some courts have refused to allow production of electronic data based on speculation or suspicion alone.

12. See Feldman & Kohn, supra note 11, at 59; see also FED. R. CIV. P. 34 (documents discoverable include "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"); Anti-Monopoly, Inc., 1995 WL 649934, at *2.
13. See FED. R. CIV. P. 26(b); MINN. R. CIV. P. 26.02.
14. See generally FED. R. CIV. P. 26(b); MINN. R. CIV. P. 26.02.
16. See FED. R. CIV. P. 26(b)(1); MINN. R. CIV. P. 26.02 (1).
17. See FED. R. CIV. P. 26(b)(2) (outlining the standard general objections to discovery); MINN. R. CIV. P. 26.02(a) (same).
18. See Mark D. Robins, Computers and the Discovery of Evidence—A New Dimension to Civil Procedure, 17 J. MARSHALL J. COMPUTER & INFO. L. 411, 413 (1999) (acknowledging that "computer-related discovery may... raise the cost of the discovery process").
19. See infra Parts II.B.2.a-b; see also MANUAL FOR COMPLEX LITIGATION § 21.433 (3d ed. 1995) (discussing the allocation of costs of discovery to the party seeking it where discovery is unduly burdensome or expensive to the other party).
20. See Alexander v. FBI, 188 F.R.D. 111, 117 (D.C. Cir. 1998) (refusing to require defendants to completely restore all deleted files and e-mail where plaintiff did not propose "targeted and appropriately worded searches of backed-up and archived e-mail and deleted hard drives for a limited number of individuals"); Fennell v. First Step Designs, Ltd., 83 F.3d 526, 531-34 (1st Cir. 1996) (affirming district court's refusal to permit plaintiff access to defendant's computer system because plaintiff had failed to offer sufficient threshold evidence of the defendant's supposed alteration and/or fabrication of evidence); Lawyers Title Ins. Corp. v. United States Fidelity & Guar. Co., 122 F.R.D. 567, 570 (N.D. Cal. 1988) (rejecting party's request to inspect the responding party's computer system where the discovering party supported its request for such access with only speculation that the responding party might not have produced relevant data);
The difference between electronic data and paper documents is that electronic data is often thought to be deleted or destroyed when, in actuality, the electronic information still exists. In addition, information about the electronic document (e.g., author of document, date and time document was created) may be imbedded in the document, which may be absent from the paper document.

In order to understand the true extent of the burden of e-discovery to companies, it is necessary to examine the types of e-data that exists in most businesses today.

1. Types of Discoverable E-Data

Electronic information can be found in anything from earlier versions and drafts of agreements or contracts, to the discovery of “deleted” e-mail that was stored on back-up tapes, to user information that is only saved with electronic data. Computers generate, sort and store incredible amounts of information that can be attractive to litigation attorneys. Additionally, computers often store information long after paper records have been destroyed. Further, a wealth of information may only be retained and stored in electronic form and, therefore, would be inaccessible if electronic data were not discoverable. It is for these reasons that litigators often focus their attention on e-data.

Often e-discovery disputes revolve around the same types of electronic media: active data, network and personal computer hard drive data, computer back-up tapes, and deleted data. All of these various media are discussed below.

a. Active Data or Data Files

When most businesses are served with discovery requests for e-data, they most likely immediately think to search their officers’ or directors’ (or other “key” actors’) personal computers for information responsive to the requests. The information that is

---

Strasser v. Yalamanchi, 669 So. 2d 1142, 1144-45 (Fla. Dist. Ct. App. 1996) (quashing a district court order permitting plaintiff unfettered access to defendant’s computer systems where plaintiff had not proven the information was retrievable).

22. See infra Part II.B.1.b.
23. See Robins, supra note 18, at 414; see infra Part II.B.1.c.
24. See Robins, supra, note 18, at 414.
readily available and accessible from these users’ personal computers is called active data or data files. Almost any kind of data can be stored as active data on a network or on personal computer hard drives. This active data can exist in the form of e-mail messages, word processing documents, spreadsheets, databases, or calendars and can be inventoried simply by reviewing the individual’s Windows Explorer or DOS file list. All of this data is subject to discovery.

“A request for raw information in computer banks is proper and the information is obtainable under the discovery rules.” Perhaps more interesting (and troubling) is that some courts have ordered parties to permit opposing counsel to physically search through their computer systems to obtain active data. There are many places, however, where responsive e-data may be found. Other data that can contain voluminous amounts of electronic information for discovering parties include replicant data, and residual data.

b. Replicant Data

A fact that may be even more startling from an e-discovery standpoint is that documents that are never saved may still “exist” and be discoverable. Most computer users have probably noticed slight pauses in processing when working in a word processing document, spreadsheet, etc. These pauses are often automatic back-ups to applications in the event of a system failure. Each time this automatic back-up occurs, a “file clone” is created and stored. These file clones create a copy (and often multiple copies) of a document or file of which the computer user probably is not even aware exists. On most networks, these file clones are saved to a

26. See Feldman & Kohn, supra note 11, at 54.
27. See id.
28. Santiago v. Miles, 121 F.R.D. 636, 640 (W.D.N.Y. 1988); see also Crown Life Ins. Co. v. Craig, 995 F.2d 1376, 1382-84 (7th Cir. 1993) (subjecting party who failed to produce properly requested raw data to sanctions even though data was not available in hard-copy form).
29. See Robins, supra note 18, at 414; Feldman & Johnson, supra note 25, at 18-21. While volume alone gets discovering parties excited, searching this voluminous data is often both extremely time-consuming for both parties as well as cost-prohibitive.
31. See id.
user’s hard drive as opposed to the network server.\textsuperscript{32} As a result of these periodic back-ups the clones continue to reside on the user’s hard drive—even after the document or file is deleted from the network server—often in multiple copies.\textsuperscript{33} In addition, data that is sent to a printer—while not saved—may be stored in a printer buffer that may also be recoverable.\textsuperscript{34} Therefore, while a user may believe he is “in the clear” because a document has been purged from the system, in reality, several copies may be residing on his hard drive.

One particularly fruitful source of replicant electronic discovery is “back-up tapes.” Back-up data is “information copied to removable media in order to provide users with access to data in the event of a system failure.”\textsuperscript{35} Backed-up copies of data may be available when systems are backed-up on either a formal or informal basis.\textsuperscript{36} Informal back-ups occur when individuals save certain documents (or even their entire hard drives) onto disk.\textsuperscript{37} Companies often will have a formal system back-up policy wherein the company’s entire computer system is “backed-up” on a regular basis—daily, weekly, or monthly—and then warehoused for a certain period of time.\textsuperscript{38} By reviewing back-up tapes created at different times, litigators may be able to assemble an electronic tale otherwise beyond their reach.

Just about any kind of e-data can be captured on computer back-up tapes. Such e-data may include executable software applications, files containing a document or spreadsheet saved in a particular application, raw data that is entered into a document or spreadsheet, and unreadable, encrypted data. Information of interest to most discovering parties contained in back-up tapes are e-mail messages, previous drafts of word processing documents, the electronic information attached to some documents, and spreadsheets with hidden columns of data and hidden notes.\textsuperscript{39}

\textsuperscript{32.} See id.
\textsuperscript{33.} See id.
\textsuperscript{34.} See Robins, supra note 18, at 418.
\textsuperscript{35.} Feldman & Kohn, supra note 11, at 54.
\textsuperscript{36.} See Feldman & Johnson, supra note 25, at 18-19.
\textsuperscript{37.} See id. at 18.
\textsuperscript{38.} See id.; Feldman & Kohn, supra note 11, at 54. Companies save archived materials for various reasons. Often, companies save this information in case of an emergency with the computer system. See Robins, supra note 18, at 416. Sometimes governmental regulation mandates record retention. See id. Other times, these materials are stored simply for historical purposes. See id. at 416 n.13.
\textsuperscript{39.} See Feldman & Johnson, supra note 25, at 18-21. See generally Charles A.
In general, a wealth of information potentially can be found in electronic documents that would not otherwise be visible in a paper copy of those same documents. For instance, many documents' file properties can reveal the date the document was created, the author of the document, subsequent edit dates to the document, which users have access to revise the document, as well as the number of versions of the document. This information, if disclosed to the opposing party, can be fodder for litigation. However, despite the value of the information, because these backup tapes potentially contain multiple copies of the same irrelevant documents, to the discovering parties' dismay, electronic data review can be an extreme waste of time and money.

c. Residual Data

Contrary to popular belief, when a computer user hits the delete button on his or her computer, the document or e-mail message "deleted" does not vanish irrevocably into thin air. Hitting the delete button merely instructs the computer to write over the hard disk space that contains that particular document, e-mail message, etc. Depending on the size and use of the computer system, it may take weeks or even months to overwrite the space containing the "deleted" information. By the time the "deleted" file is actually overwritten, the "deleted" item may have been backed-up many times over for retrieval at any moment. Additionally, sometimes "deleted" files are only partially overwritten which enables competent computer forensic experts to recover the remaining parts of the document.

Lovell & Roger W. Holmes, The Dangers of E-Mail: The Need for Electronic Data Retention Policies, 44 R.I. B.J., Dec. 1995, at 7-8 (discussing the ramifications of discovering unrestrained statements in e-mail and other documents). Draft contracts often disclose attorneys' mental impressions and reveal potential legal issues regarding certain language in the contract, making the discovery of such information potentially dangerous. See id.

40. See Robins, supra note 18, at 415. Computer forensic experts can easily recover prior drafts of documents. See Lovell & Holmes, supra note 39, at 8.
41. See Lovell & Holmes, supra note 39, at 8.
42. See Robins, supra note 18, at 417.
43. See id.
44. See id.
45. See supra Parts II.B.1.b-c (discussing documents which are stored on hard drives and computer back-up tapes).
46. See Lovell & Holmes, supra note 39, at 8.
d. E-Mail

E-mail potentially can be a great source of evidence for the opposing party in litigation because people generally use e-mail as a way to communicate informally or candidly. E-mail is among the most popular mode of communication in the workplace. Currently, an estimated 108 million people are believed to be e-mail users, doubling the number of users in just four years, and that number will only continue to increase throughout the twenty-first century. Usually e-mail composers fail to take much care and consideration when creating an e-mail message. What most e-mail users do not realize, is that e-mail messages are more likely to be permanent than paper letters. For instance, as discussed above, simply using the “delete” key on a keyboard does not permanently erase an e-mail message. Further, e-mail is very easy to duplicate and forward; therefore, e-mail can easily end up in the possession of an unintended recipient. Finally, if a business runs periodic back-ups of their network, e-mail messages are “backed-up” and stored on back-up tapes, making the messages everlasting (or at least as long lasting as the back-up tape).

Another troubling factor regarding e-mail usage is that many businesses do not provide e-mail usage training or promote an e-mail usage policy. Therefore, not only can e-mail users use e-mail for non-business purposes without fear of punishment, presumably they can use e-mail for purposes that expose employers to

---

47. While e-mail can be any of the three types of data discussed above (i.e., active, replicant or residual), the authors believe that e-mail is important enough to the e-discovery discussion to warrant its own section.


49. See Feldman & Kohn, supra note 11, at 56.


51. See Enzinna, supra note 48, at 47-48.

52. See supra Part II.B.1.b. (discussing the creation of back-up copies of documents).

53. See supra Part II.B.1.c.

54. See Enzinna, supra note 48, at 47-48.

55. See Feldman & Johnson, supra note 25, at 18-21.

56. See Feldman & Kohn, supra note 11, at 56 (stating that a recent survey revealed that 49% of organizations using e-mail did not train their employees on e-mail use and 48% of the organizations using e-mail did not have an official e-mail policy).
substantial liability. While e-mail has most definitely had positive effects on the business environment, it also creates its share of headaches. One of the most notable downsides to e-mail has been its increase in the amount of information subject to discovery in litigation. This has never been more evident than in the recent Microsoft antitrust litigation. Even more in the public eye are the e-mail debacles that are currently plaguing the White House.

57. See infra Part III.A.2. (discussing necessity of e-mail usage policies); see also Feldman & Kohn, supra note 11, at 56 (noting that 22% of organizations using e-mail and responding to a survey stated that they had received complaints about offensive e-mail messages).

58. See Enzinna, supra note 48, at 47-48. Specifically, e-mail (1) increases the amount of information subject to discovery; (2) increases the costs associated with discovery; (3) can be damaging; (4) can subject employers to liability; and (5) may imperil privileges. See id. at 48-51.

59. In the Microsoft case, a small software company used internal Microsoft e-mail to prove its private antitrust claims against the computer software giant. Caldera, Inc. used Microsoft e-mail as evidence showing that top Microsoft executives plotted to rig Caldera's software to make the software incompatible with competing operating systems. See Leslie Helm, E-Mails Show Gates, Others Plotting to Thwart OS Rivals Courts: Caldera offers dramatic evidence to back its claims in a private antitrust action against Microsoft, L.A. TIMES, Apr. 29, 1999, at C1. In a December 1989 e-mail, Microsoft CEO Bill Gates wrote “[MS]-DOS remains the backbone . . . of both our software businesses. It is under extreme attack by high-quality clones like DR-DOS.” Id. Gates questioned in a follow-up e-mail whether it would be possible to make Microsoft's software applications work with MS-DOS, yet be incompatible with the DR-DOS operating systems. See id. In yet another e-mail, Gates apparently ordered Microsoft programmers to make it seem as if Microsoft's software was incompatible with DR-DOS by displaying an error message when a user used a DR-DOS platform. See id.

In another instance, the U.S. Department of Justice used embarrassing e-mail from Gates in the government's antitrust investigation into Microsoft. See Associated Press, Government Wraps Up Microsoft Case Prosecutors Use Embarrassing E-Mail, Video of Gates to Make Antitrust Point, ORLANDO SENT., Jan. 14, 1999, at C5. Just prior to resting its case-in-chief, the Justice Department released more than 1,000 pages of new evidence relating to Bill Gates' sworn testimony—most of which was e-mail. See id.

Finally, while Gates steadfastly denied discussion of a cooperative agreement between Microsoft executives and Netscape officials, e-mail from one Microsoft executive summarized the meeting with Netscape stating “[w]e need to understand if you will adopt our platform and build on top of it or if you are going to compete with us on the platform level.” James V. Grimaldi, The Gates Deposition: 684 Pages of Conflict, SEATTLE TIMES, Mar. 16, 1999, at A1.

60. In February 2000, a Washington Times article revealed that up to 100,000 e-mail messages had not been produced by the White House despite being sought by several subpoenas from investigators looking into “Filegate,” “Chinagate,” the Monica Lewinsky affair, and other matters. See Legacy of Lawlessness, WASH. TIMES, Feb. 18, 2000, at A20. These e-mails where allegedly inadvertently misplaced. See George Lardner, Jr., E-mail Probe Was Expected; White House Recovery Plan Awaited
2. Limitations of E-Discovery

Although courts are generally accepting the notion of the discovery of e-data, they have, in some instances, imposed noteworthy limitations. These limitations are addressed below.

a. Overbroad and Unduly Burdensome Objection Successful

When faced with an e-discovery request, the best way to limit the scope of an electronic discovery search obligation is to assert that such a search is overly broad and unduly burdensome. Many courts have limited e-discovery requests based on the overbroad and unduly burdensome objections. "[C]ourts will generally not require a company to submit to intrusive, expensive or burdensome discovery of their electronic files where the burden is not justified..."

Inquiries From Hill, WASH. POST, May 2, 2000, at A21. The White House is expected to produce the misplaced e-mails within the next six months. See Don Van Natta, Jr., Former Counsel Takes Responsibility for Missing E-mails, N.Y. TIMES NEWS SERV., May 5, 2000. The price tag on the White House's restoration of the missing e-mails from back-up tapes is $3 million. See id.

61. See supra Parts II.A and B.

62. See FED. R. CIV. P. 26(c). Rule 34 does not provide for unfettered access to discovery. See generally Belcher v. Bassett Furniture Indus., Inc., 588 F.2d 904, 906-07 (4th Cir. 1978) ("Granting or denying a request under rule 34 is a matter within the trial court's discretion, and it will be reversed only if the action taken was improvident and affected substantial rights.") (citing Tiedman v. American Pigment Corporation, 253 F.2d 803, 808 (4th Cir. 1958)).

63. See Fennell v. First Step Designs, Ltd., 83 F.2d 526, 534 (1st Cir. 1996) (affirming district court's decision not to permit access to a party's hard drive in order to investigate the date on which a document had been created or modified); Van Westrienen v. Americontinental Collection Corp., 189 F.R.D. 440, 441 (D. Ore. 1999) (holding that "Plaintiffs are not entitled to unbridled access [of] defendants' computer system. Plaintiffs should pursue other less burdensome alternatives, such as identifying the number of letters and their content"); Symantec Corp. v. McAfee Assocs., Inc., No. 97-20967, 1998 WL 740807, at *3-4 (N.D. Cal. Aug. 14, 1998) (holding that plaintiff's request for the production of copies of all hard drives that had access to a specific server was unduly burdensome); Strasser v. Yalamanchi, 669 So. 2d 1142, 1144-45 (Fla. Dist. Ct. App. 1996) (holding that while plaintiff's request to search defendant's computer system was within the scope of Florida's discovery rules, the inspection sought by the plaintiff was overly broad since the order sought by the plaintiff would have given the plaintiff unfettered access to defendant's entire computer systems which could cause defendant irreparable harm); In re Brand Name Prescription Drug Antitrust Litig., No. 94-987, 1995 U.S. Dist. LEXIS 8281, at *7-8 (N.D. Ill. June 13, 1995) (narrowing broad requests of plaintiffs and requiring parties to agree upon meaningful limitations on the scope of any e-mail search); In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993, 846 F. Supp. 11, 13-14 (S.D.N.Y. 1994) (quashing a grand jury subpoena for all computer hard drives and floppy disks as unreasonably broad).
by the relevance of the evidence likely to be discovered, the size of the case and the availability of less burdensome alternatives for obtaining the information.”

b. Cost as Basis for Objection

As a component of the burdensome objection, courts have also examined cost issues. Where the discovery is unduly burdensome or expensive and the parties’ resources are disproportionate, the possibility exists for a court to order an allocation of costs. However, in most cases, the party required to produce the e-discovery is often the party required to pay for the production.

Copy costs of electronic data, however, are generally borne by the requesting party—not the producing party. Likewise, if response to discovery requests requires extraordinary measures to


65. See Manual for Complex Litigation § 21.433 (3d ed. 1995) (citing FED. R. CIV. P. 26(b)(2) & (c)). Some courts may shift the burden and costs of the production from the producing to the requesting party. See, e.g., Oppenheimer Funds, Inc. v. Sanders, 437 U.S. 340, 342 (1978) (holding that Federal Rule of Civil Procedure 23(d) empowers a court to direct the requesting party to bear production burdens and costs in a class action).

66. See Sattar v. Motorola, Inc., 138 F.3d 1164, 1171 (7th Cir. 1998) (affirming district court’s decision to allow defendant to download 210,000 pages of e-mail messages into a readable format disk as opposed to printing out the same, or alternatively, requiring defendant and plaintiff would have to split costs of paper printouts if e-mail was not readable in downloadable form); Brand Name Prescription Drugs Antitrust Litig., 1995 U.S. Dist. LEXIS 8281, at *5 (holding defendants responsible for $50,000-70,000 cost of searching 30 million pages of archived e-mail messages where procedure was the product of defendants’ own record-keeping); Bills v. Kennecott Corp., 108 F.R.D. 459, 463-64 (D. Utah 1985) (denying defendant’s request that plaintiff pay costs of production of computer data from defendant’s computer because the cost was not excessive and the burden of the plaintiff in obtaining the data would be substantially greater); Linnen v. A.H. Robins Co., Inc., No. 97-2307, 1999 WL 462015, at *12 (Mass. Super. Ct. June 16, 1999) (holding that producing company must bear costs incurred). But see O’Meara v. IRS, No. 96-C-7276, 1997 WL 312054, at *1 (N.D. Ill. June 5, 1997) (denying plaintiff’s request to require IRS to conduct expansive search of its databases at agency’s expense); Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94 Civ. 2120LMMAJP, 1996 WL 22976, at *2-3 (S.D.N.Y. Jan. 23, 1996) (rejecting plaintiff’s argument that it was too impoverished to bear defendant’s costs of creating computer programs used to extract requested data from the defendant’s databases).

comply, such costs are generally required to be paid by the requesting party. 68

c. Attorney-Client Privilege and Work Product Objections Still Apply

While the discoverability of e-data can be a great breakthrough for the discovering party, it can be a nightmare to the producing party for the reasons discussed above. In addition to the disclosure of factual information, producing parties also need to be cognizant of potential privilege issues when producing their e-data. Like standard paper document discovery, documents stored on back-up tapes or computer hard drives may contain privileged attorney-client information and/or attorney work product. 69 Courts have recognized the need to preserve the attorney-client privilege and work product doctrine objections in the production of e-discovery. 70

Before producing back-up tapes in their entirety, data must be reviewed for these potential privilege issues. 71 As in the non-electronic discovery context, this privilege can be inadvertently waived. 72 One way to easily limit the review of a massive amount of documents is to search the data for specific identifiable terms that are relevant to the issues of the litigation. 73 For instance, when searching for privileged documents, a search could be conducted containing all attorneys’ names. 74 Although such a search may be a

68. See Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050, 1054 (S.D. Cal. 1999) (requiring the requesting party to bear costs of having forensics expert make mirror image of defendant’s hard drive); see also Oppenheimer Funds, Inc., 437 U.S. at 386.
69. See Robins, supra note 18, at 421.
71. See Robins, supra note 18, at 421.
73. When conducting word searches generally, the attorney can work with opposing counsel to agree on a list of relevant terms for conducting the search. Experienced local and national technology companies can assist in this effort.
74. One caveat to this approach is that a hastily conducted search can turn up many “miss-hits.” For example, a word search for an attorney with the last name
more efficient manner in which to conduct a privilege review, a risk still exists that the search will not identify all privileged documents and an inadvertent production may occur.

III. PRACTICAL APPLICATIONS: GETTING CLIENTS IN THE BEST POSITION TO DEAL WITH LEGAL ISSUES SURROUNDING E-DISCOVERY AND THE TECHNOLOGY AGE

Considering the new playing field lawyers and clients are facing and the line of court cases sympathetic to the requesting party's right to obtain relevant documents, counsel and their clients must efficiently and expeditiously address these issues. Efficiency will stem from: (1) taking prudent business steps to organize the company's electronic storage efforts; (2) implementing relevant document retention, employee Internet and e-mail usage policies; and (3) taking immediate "preservation" steps at the outset of litigation. If these steps are taken, a company's chances of avoiding a litigation discovery nightmare increase dramatically.

A. Counseling Your Clients Prior to Litigation: Steps Companies Should Take Before (and Even to Avoid) Being Sued

1. Trouble Clients Want to Avoid

Today, e-mail and Internet access are available from the computer desktops of most corporate employees in America. Although these tools provide the benefits of efficient communication and ease of access to a wealth of information, they also provide fertile ground for abuse by employees—which can lead to corporate legal exposure in employment-related and other disputes and to the unchecked creation of a litigation "paper trail"

"Berg" could produce hundreds of other names such as Greenberg or Rosenberg or other nouns such as iceberg, if not conducted prudently. No search is foolproof, but some critical thought should be given when choosing search terms.

75. E-discovery obviously poses issues for both parties and their respective counsel. This article attempts to address the issues solely from the defense perspective. For articles discussing the offensive use of e-discovery, see Feldman & Kohn, supra note 11, at 53; Jay E. Grenig, Electronic Discovery: Making Your Opponent's Computer a Vital Part of Your Legal Team, 21 AM. J. TRIAL ADVOC. 293, 293 (1997); Peter V. Lacouture, Discovery and the Use of Computer-based Information in Litigation, 45 R.I. B.J., Dec. 1996, at 9.

76. See infra Parts III.A.2.a-b.

77. See infra Part III.B.
management may not even know exists. 78

a. Employment Litigation

Using e-mail and the Internet at work, employees may send harassing, pornographic or other inappropriate “jokes” or messages. As with other verbal comments or hard copy “jokes,” these messages are no joking matter to many recipients. The result—lawsuits. Employees’ improper use of e-mail and the Internet has resulted in the discovery of and use of electronic evidence in a large number of employment related disputes, including wrongful termination, 79 employment discrimination 80 and sexual harassment. 81 From a risk management and human

78. Employee access to e-mail and the Internet also poses enormous productivity concerns for employers. See generally Stuart J. Kaplan, E-Mail Policies in the Public Sector Workplace: Balancing Management Responsibilities with Employee Privacy Interest, 15 LERC MONOGRAPH SERIES 103, 114 (1998) (discussing both potential risks to employers of improper employee email usage and productivity issues); Thomas P. Klein, Electronic Communications In the Workplace: Legal Issues and Policies, 563 PLI/PER 695, 714 (1999) (emphasizing that employers should implement strict policies concerning employee use of employer’s e-mail systems and the internet).

79. See, e.g., Daniels v. Worldcom Corp., No. CIV.A.3:97-CV-0721-P, 1998 WL 91261, at *1 (N.D. Tex. Feb. 23, 1998) (stating that plaintiffs alleged that a co-worker sent e-mails containing offensive racial jokes, that they had complained about the messages, and as a result, their manager retaliated against them).

80. See, e.g., Owens v. Morgan Stanley & Co., No. 96CIV.9747, 1997 WL 403454, at *1 (S.D.N.Y. July 17, 1997) (stating that plaintiffs alleged that a Caucasian co-worker sent an e-mail message containing racial jokes to other Caucasian employees, and as a result of reporting the e-mail to supervisors, plaintiffs were denied promotions and were socially ostracized); Strauss v. Microsoft Corp., No. 91-5928, 1995 WL 326492, at *4-5 (S.D.N.Y June 1, 1995) (permitting certain statements and e-mail messages proffered by plaintiff in a sex discrimination case to be admissible at trial).

81. See, e.g., Yamaguchi v. U.S. Dept. of the Air Force, 109 F.3d 1475, 1477 (9th Cir. 1997) (involving allegations of Title VII sexual harassment including offensive e-mail messages); Knox v. State, 93 F.3d 1327, 1330, 1334 (7th Cir. 1996) (stating that an employee was successful in bringing a Title VII sexual harassment action against the State of Indiana where her allegations included a supervisor sending her sexually suggestive electronic messages); Rudas v. Nationwide Mut. Ins. Co., No. 96-5987, 1997 WL 11302, at *1 (E.D. Pa. Jan. 10, 1997) (involving graphic e-mail messages used to support allegation of sexual harassment); Huffman v. Pepsi-Cola Bottling Co., No. C7-94-2404, 1995 WL 434467, at *1 (Minn. Ct. App. July 25, 1995) (involving sexually explicit computer games on company computers as part of allegations of sexual harassment); Dennis v. Carroll City Dep’t of Human Serv., No. 442, 1993 WL 19622, at *1-3 (Ohio Ct. App. Jan. 28, 1993) (finding that the evidence of plaintiff’s behavior and numerous advances, including evidence of e-mails plaintiff had sent, was sufficient to support a finding of sexual harassment).
relations standpoint, these are obviously situations that an employer would like to be able to monitor and eliminate.

b. Examples of E-Discovery in Other Litigation

E-mail has been the cause of costly litigation and embarrassment in other situations as well. For example, in Siemens Solar Industries v. Atlantic Richfield Co., a highly publicized case, Siemens entered into a stock purchase agreement with ARCO. Siemens filed suit against ARCO alleging that ARCO had made false representations relating to the viability of ARCO's TFS technology system. Through discovery, Siemens uncovered the proverbial smoking gun—internal ARCO e-mail messages between ARCO and ARCO Solar representatives that revealed ARCO's opinion that TFS production was, indeed, not commercially viable.

Perhaps the most highly publicized and ironic example of e-mail damaging a corporation is the Microsoft antitrust litigation. During the Microsoft litigation, Bill Gates, in a sworn deposition, flatly contradicted his e-mail statements, and an e-mail from James Barksdale, chief executive of Netscape, to America Online's chairman, Steve Case, in which he referred to Case as "Franklin D." and himself as "Joseph Stalin" in an allusion to the leaders of the United States and the Soviet Union in World War II. These examples of cavalier e-mail use should be reason for concern and the impetus for proactivity with respect to electronic document issues for all companies.

2. How to Help Your Client Protect Itself From Trouble

Obviously, not all "trouble" can be avoided. Certainly, management cannot completely control the use and content of electronic communication by its employees. However, there are

83. See id. at *2.
84. See id.
85. See id. One ARCO e-mail stated something to the effect of "it appears [the technology] is a pipe dream, let Siemens have the pipe." Id.
86. See supra note 61 and accompanying text (discussing the Microsoft e-discovery situation in detail).
87. See Amy Harmon, E-Mailers Tighten Up Loose Lips; Companies, Citing Legal Concerns, Curb Electronic Messages, INT'L HERALD TRIB., Nov. 12, 1998; see also supra note 59 (discussing other damaging e-mails in the Microsoft antitrust trial).
steps companies can take to minimize risk and control the universe of documents that may be discovered, and potentially used against the company in litigation.

a. E-Mail and Internet Policies

Companies whose employees use electronic communications media should develop policies and procedures to minimize non-productive e-mail and Internet use while, at the same time, protect the corporation’s interests. E-mail and Internet use policies should be well thought out and tailored to address the concerns of the particular business. Although policies will vary with the type of business, companies should consider addressing the following issues, in clear and concise fashion, in their policies:

1. the extent of usage allowed—specifically state the restrictions on the use of e-mail and the Internet;
2. inform the employee that the employer’s computer, technology and communications system, including e-mail and the Internet, are the sole property of the employer;
3. inform the employee no e-mail message is considered private, except where it may benefit the company, and that employees should not expect that their messages will remain private;
4. a statement that the company reserves the right to monitor usage of e-mail and the Internet, in the ordinary course

88. See generally Lovell & Holmes, supra note 39, at 7-8 (discussing the need for e-mail policies and citing examples of devastating e-mail discoveries). According to the American Management Association, in 1999, at least 45% of employers said that they monitor their employees’ computer files and e-mail. See Lisa Guernsey, The Web: New Ticket to a Pink Slip, N.Y. TIMES, Dec. 16, 1999, at G1.

89. There may be privacy concerns with monitoring employee e-mail and Internet usage. See generally Electronic Communications Privacy Act of 1986 (codified at 18 U.S.C. §§ 2510-2522 (1994)); Minnesota Privacy of Communications Act (codified at MINN. STAT. § 626A.01-.41 (1998)). Moreover, after a long history of refusing to recognize a cause of action based on privacy interests, the Minnesota Supreme Court finally joined the almost unanimous ranks of the other states by recognizing tort claims relating to the right to privacy in Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231 (Minn. 1998) (recognizing privacy causes of action for intrusion upon seclusion, appropriation and publication of false facts, but refusing to recognize claims for false light publicity). This article does not purport to address these privacy concerns in detail. For an article discussing the privacy issue, see, for example, Reginald C. Govan, Confidentiality of Personal Information, Communications Made Through Electronic Information Systems, and Internal Investigative Records, 600 PLI/LIT 883, 895-900.
of business; and
5. the prohibition against using e-mail or the internet to communicate harassing, offensive, defamatory or sensitive messages, including, but not limited to, messages inappropriate under the company’s harassment and other policies.90

Companies may also want to consider having the policy include the following prohibitions:

1. solicitation or proselytizing for charitable, religious, political or other non-business purposes;
2. transmission of trade secrets, confidential or privileged communications;
3. the unauthorized copying and distribution of copyrighted material; and
4. uses, such as chain mail, that degrade system performance.91

In order to ensure compliance, employers must communicate or disseminate policies directly to the employees.92 The policies should also contain information concerning the consequences93 of violating the policies.94 Employees should be required to sign an acknowledgment that they have read, understand and agree to abide by the policy and its terms.95 Periodic reminders of the policy and necessity of compliance are also encouraged.96

b. Electronic Data Retention Policies

Although the advent of technology has in some sense saved “physical space” with respect to document storage, as the use of technology increases, a company’s computer storage space will be

---

90. See Peter Brown, Developing Corporate Internet, Intranet and E-mail Policies, 520 PLI/PAT 347, 363 (1998); see also MINNESOTA DEP’T OF TRADE AND ECON. DEV. & MERCHANT & GOULD, P.C., A LEGAL GUIDE TO THE INTERNET 75 (1999).
91. See Brown, supra note 90, at 363-64.
92. See id. at 357.
93. Consequences for violation of the policy can be severe. For example, according to a recent New York Times article, Xerox fired 40 employees who had been “caught in the act” (by monitoring software) of surfing forbidden websites. See Guernsey, supra note 88, at G1.
94. See Brown, supra note 90, at 369.
95. See id.
96. See id.
taxed as well. Like paper documents, there is certainly no need to
retain every electronic document, e-mail, memorandum, or letter
indefinitely. However, there are business reasons and legal
requirements imposed by statutes and regulations that mandate
maintenance of certain types of records. To effectively manage
these competing concerns, companies should consider
implementing a document retention program that encompasses all
of its records, electronic and otherwise. Many companies already
have document retention policies for their "paper" documents.

A document retention policy "involves the systematic review,
retention, and destruction of documents received or created in the
course of business." One author suggests that the decision to
implement such a program must take into account the "balancing
of potentially competing interests," including "(1) legal obligations,
(2) efficiency considerations, and (3) pre-litigation concerns." There is no template policy, as each company's policy must be
tailored to its specific needs. A document retention policy
should be grounded in legitimate business objectives and not a
basis for destroying documents which may be potentially relevant to
later litigation.

As part of its document retention program, a company should
specifically address concerns with respect to electronic documents,
particularly e-mail. As part of their routine practice, companies
should consider using computer programs that electronically
remove deleted messages so that they can no longer be retrieved.
Companies should also index e-mail archives in order to allow for
efficient searching when required. Companies may also consider
adopting policies intending to delineate official company e-mail,
which should be treated as a paper document and subject to
regular document retention policies, and personal unofficial e-mail,

97. See Christopher V. Cotton, Document Retention Programs for Electronic
Records: Applying a Reasonableness Standard to the Electronic Era, 24 J. Corp. L. 417,
419-20 (1999) (detailing various types of legal record retention policies).
98. See Lovell & Holmes, supra note 39, at 8.
99. Cotton, supra note 97, at 419.
100. Id. (explaining in detail these three concerns).
101. See id. at 421-22 (detailing the general components of a records retention
policy). This article does not purport to address all concerns in implementing a
record retention policy. Its focus is merely on the general issues to consider with
respect to electronic documents.
102. Certainly, if litigation commences or is imminent, the policy may need to
be temporarily stayed to prevent destruction of potentially relevant documents.
103. See Brown, supra note 90, at 367.
which should be routinely deleted. Some companies have assigned employees two separate e-mail accounts, one for official business and another for personal and/or administrative communications. At a minimum, corporations should consider including the following in their corporate e-mail retention policies:

1. A statement specifying the routine deletion of e-mail after a specified time.
2. A statement requiring employees to discard their e-mail regularly and a limit on the space allotted to each employee for their e-mail. The company can use computer programs that automatically purge inactive e-mail.
3. A statement that the automatic deletion of electronic records will be suspended and steps taken to preserve these records once litigation or a formal investigation is commenced.

Following the above-delineated steps should put a company in a better position to respond to discovery requests and defend itself in litigation. A company will also find itself better organized from a business perspective.

B. Steps To Take When Your Client Has Been Sued

Although courts have not been uniform in their approaches as to the duty to preserve documents and information, many courts have held that the parties have an obligation to preserve documents and information (electronic and non-electronic) that is reasonably foreseeable to be relevant to potential or ongoing litigation. Failure to do so may result in liability for spoliation of

105. Brown, supra note 90, at 367.
106. A document retention policy may also provide a defense to a charge that a company wrongfully destroyed a document. A company can potentially avoid an adverse inference against it for destruction of a document if it can establish that the destruction occurred in good faith, subject to a bona fide document retention policy. See generally Lewy v. Remington Arms Co., Inc., 836 F.2d 1104 (8th Cir. 1988) (outlining factors used to determine if a document retention policy is reasonable).
evidence,\textsuperscript{108} exclusion of evidence,\textsuperscript{109} or in a default judgment as a discovery sanction.\textsuperscript{110} Once a lawsuit is filed (or the company has reason to believe it is likely to be filed), the company should take steps to ensure the preservation of the universe of relevant documents and information.\textsuperscript{111} Once an attorney is retained to represent the company in the lawsuit, the attorney should work closely with the general counsel or other designated management personnel to establish a document preservation protocol. This protocol should include: an identification of the potentially relevant corporate “key” actors and the potentially relevant universe of documents with respect to each “key” actor. Depending on the size of the company and the nature of the dispute, the attorneys may need to coordinate with the company’s internal information services or technology department to develop an understanding of the company’s technology, document retention policy and practices, the company’s policy with respect to back-up tapes, and whether any relevant tapes exist and to establish a protocol for addressing these issues with respect to discovery. All of these steps should be documented. Taking these steps at the outset of litigation will simplify the actual discovery and document production process. Furthermore, it serves as evidence of a company’s good faith and reasonable response to discovery.\textsuperscript{112}

\textsuperscript{108} See Robins, \textit{supra} note 18, at 421. In implementing its document retention policies, companies should use care to avoid being overly aggressive in purging computer records. See \textit{id}. An overaggressive approach may lead to a charge of spoliation. See \textit{id}.

\textsuperscript{109} See Townsend, 174 F.R.D. at 4 (noting potential sanctions can be: dismissal of case, exclusion of evidence, or a jury instruction on the “spoliation inference”). The court can apply a “negative inference” that the destroyed document would be favorable to the party who failed to produce it. See generally Kmetz v. Johnson, 261 Minn. 395, 403, 113 N.W.2d 96, 101 (1962) (“[W]ith respect to documentary evidence, that some effort must be made by a party to obtain this type of evidence from an opponent before an unfavorable inference can be drawn against the opponent for failure to produce it.”).


\textsuperscript{111} This may include making exceptions to the company’s document retention policy.

\textsuperscript{112} Failure to take these types of steps and produce documents reasonably encompassed by discovery requests may result in the court requiring the expensive restoration of back-up tapes.
C. How to Conduct A Reasonable Good Faith Discovery Search

The process one must go through to respond to an electronic discovery request is not all that different from responding to a standard document request. The party must identify: the "key" internal personnel who may have relevant information, the types of documents and information that may be relevant, and the potentially relevant time period. From there, in addition to the hard copy document search, the following steps should be taken to search for potentially relevant documents:

1. Search each "key" person's:
   a. office computer hard drive;
   b. laptop computer;
   c. home computer (if used for business purposes);
   d. handheld computer devices (e.g., Palm Pilots);
   e. network files;
   f. a-e for each key person's assistant or staff;

2. Produce any individually "backed-up" data, such as floppy disks.

If the nature of the lawsuit is such that relevant documents are known to have been purged from the above-listed sources under the company's document retention policy, it may be necessary to search system back-up tapes (if any exist) for relevant documents. The company and its counsel should document the steps taken above as well.

If each of these steps is followed, the company should be on solid ground that it has fulfilled its discovery obligations.

114. See id. at *2.
115. See Feldman & Kohn, supra note 11, at 65.
116. See supra Part II.B.1.b. In the event that back-up tapes must be restored, there are companies that specialize in this type of work. At this point, the parties should meet to agree upon a protocol for the restoration of the data in order to minimize costs and limit the restoration to relevant, usable data. The use of relevant search terms may be helpful to limit the universe of documents that need to be reviewed for production.
117. As case law develops (and potentially separate e-discovery rules develop), a party's discovery obligations will be further defined.
D. Situations To Avoid: The Litigation Nightmare

The unwary company that does not utilize a proactive approach to document and data management, as outlined above, may find itself in an expensive litigation nightmare. These nightmares can range from hefty sanctions and/or the entry of default to being ordered to engage in an expensive electronic information restoration process.118

A company's failure to produce e-discovery has proven to be costly and has resulted in the ordering of sanctions and default judgment. One example of this notion is a recent case, Proctor & Gamble Co. v. Haugen,119 where Proctor & Gamble was sanctioned $10,000 for failing to retain and produce e-mail of five key employees.120

Another example is Crown Life Insurance Co. v. Craig,121 where the Seventh Circuit upheld the district court's default judgment sanction against the defendant for failure to produce relevant electronic documents and information in response to the plaintiff's general document requests.122

One final telling example of an expensive restoration process is in Linnen v. A.H. Robins Co., Inc.,123 a case that presents a situation defense lawyers and their clients will surely want to avoid. The

---

118. See generally supra notes 108-10, and accompanying text (discussing consequences of inadequate document retention and production).
120. See id. at 632. In Proctor & Gamble, Proctor & Gamble (P & G) filed suit against two distributors of Amway products. See Proctor & Gamble, Co. v. Haugen, 947 F. Supp. 1551, 1553 (D. Utah 1996). Although Amway was not a named party, P & G served a subpoena duces tecum to discover 30 broad categories of documents, including e-mail. See id. The subpoena admonished Amway to not destroy its electronic data. See id. Some months later, Amway was added as a party to the lawsuit by P & G. See Procter & Gamble, 179 F.R.D. at 622. For many reasons, the subpoena was unduly burdensome for Amway and the two companies attempted to negotiate a resolution. Because the parties were unable to reach an agreement, Amway moved for a protective order and was largely unsuccessful. See id. at 632-33. Upon conducting discovery, Amway learned that despite P & G's strict admonition to Amway to retain its e-mail, P & G failed to retain its own e-mails. See id. at 631. The minimal backup of P & G's system that did occur did not include five key employees designated by P & G as having relevant information. See id. at 632. The resulting discovery produced no electronic documents on the system during the time frame of the events leading to the lawsuit. See id. Amway filed a motion for sanctions. See id. The court ordered P & G to pay Amway $10,000 for its bad faith destruction. See id.
121. 995 F.2d 1376 (7th Cir. 1993).
122. Id. at 1383-84.
*Linnen* case was a state court wrongful death action dealing with the infamous weight-loss drug fen/phen. 124 The central issue in the case was the defendant's knowledge of the risks of the product. 125 Plaintiffs sought discovery of any electronic mail messages retained by Wyeth-Ayerst Laboratories (Wyeth) that were responsive to the plaintiffs' discovery requests. 126 Not surprisingly, Wyeth opposed such discovery, claiming it had already produced a large number of documents, including e-mail messages. 127 Further, Wyeth objected on the grounds that it would be unduly burdensome and costly for it to restore the back-up tapes containing the e-mail and other documents. 128 Moreover, if ordered to produce such information, Wyeth requested that the plaintiffs be compelled to absorb the cost. 129

The plaintiffs in *Linnen* became interested in the discovery of e-mail when they learned through discovery that many Wyeth employees had used e-mail to communicate regarding the issues that were the subject of the lawsuit. 130 The plaintiffs then specifically requested e-mail sent or received by fifteen individuals on several topics for a certain time period. 131 Wyeth responded that it had "no mass storage devices' or other back-up tapes containing electronic mail messages" for that period. 132 However, Wyeth was able to produce e-mail messages saved on personal computers. 133 Several months later, Wyeth became aware that it had back-up tapes in storage that could contain responsive information. 134 As it turned out, Wyeth located over one thousand back-up tapes from a variety of software systems. 135 Five categories of tapes existed, including over one thousand tapes from the relevant time period. 136 The cost to restore one category of the tapes ranged between $300,000 to $350,000 and $850,000 to $1.4 million for another—

124. See id. at *1.
125. See id.
126. See id. at *2.
127. See id. at *1-2.
128. See id. at *1.
129. See id.
130. See id. at *2.
131. See id.
132. Id.
133. See id.
134. See id. at *3-4.
135. See id. at *4.
136. See id.
137. See id.
an obvious ground for the undue burden objection.

Rather than order a wholesale restoration, the Court held that it would await the outcome of the protocol endorsed in the Federal Court Multi-District Litigation (MDL), wherein Wyeth, also a defendant in the MDL, agreed in that case to restore a sampling of tapes from each of the categories which were identified as possibly containing relevant information. Under the MDL protocol, Wyeth would bear the initial costs but had the right to seek reimbursement of up to $25,000 from the plaintiffs. Only upon a showing of good cause would further production be required. Pending the findings in MDL, the Court in Linnen left open the issue for re-evaluation.

Of particular interest to future corporate defendants was the Massachusetts court’s comment in Linnen:

[T]his is one of the risks taken on by companies that have made the decision to avail themselves of the computer technology now available to the business world. To permit a corporation such as Wyeth 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.

These are just a few examples of litigation nightmares. Undoubtedly, more will follow as companies begin to realize the perils of technology in the litigation context.

IV. CONCLUSION

Technology has changed the face of the business world. As discussed above, although this technology is beneficial in many respects, it is also a source of potential liability for companies. Courts repeatedly allow discovery of electronic data. Although access to such information is not without limitations, the practical reality is that electronic discovery will inevitably play a part in all

138. The MDL is a consolidated suit brought by thousands of plaintiffs alleging injury as a result of diet-related pharmaceutical products. See id.
139. See id. at *5.
140. See id.
141. See id.
142. See id. at *6.
143. Id. (internal citation omitted).
types of litigation now and into the future.

The laundry list of e-discovery horror stories continues to grow. With that in mind, companies must adapt to this changing landscape to put themselves in the best position possible to tackle such difficult and cutting-edge legal issues presented by this new medium and to enable them to not be the next example of an electronic discovery nightmare. While all "trouble" certainly cannot be avoided, attorneys can work with their clients to assist them in protecting themselves. Useful pre-litigation tools that all companies can use to protect themselves include the implementation of e-mail, Internet and electronic data retention policies. Once litigation commences, companies can protect themselves by implementing steps to preserve the universe of relevant data and to enable them to conduct an efficient, good faith reasonable search that both comports with their discovery obligations in response to discovery requests aimed at electronic evidence and does not necessitate excessive and unnecessary expense to the company.

Although it is well-established that electronic data is discoverable, the law continues to be developed with respect to e-discovery. As technology continues to evolve, businesses will undoubtedly be faced with many new and difficult issues. For now, attorneys can assist their clients by counseling them with respect to the potential pitfalls and by assisting them in implementing preventative systems to protect themselves against such issues.