William Mitchell Law Review

Volume 27 | Issue 3 Article 2

2001

The Discovery of Electronic Data in Litigation: What Practitioners and Their Clients Need to Know

Devin Murphy

THE DISCOVERY OF ELECTRONIC DATA IN LITIGATION: WHAT PRACTITIONERS AND THEIR CLIENTS NEED TO KNOW

Devin Murphy†

I. INTRODUCTION

Each day, more and more people and businesses are relying upon computers to communicate and process information. Current estimates show that thirty-five percent of corporate communi-

† J.D. expected May 2001, William Mitchell College of Law.

cations take place electronically.[1] Furthermore, estimates expect U.S. workers will send more than twenty-five billion e-mail messages each day in 2000.[2] In fact, one commentator reports that employees of Kodak send two million e-mail messages each day.[3] Not only is electronic communication booming, the Internet is fast becoming a major source of information and business opportunity.[4]

Knowing that electronic data is created and processed in astronomical numbers, why should attorneys be concerned? First, electronic data is discoverable. The Federal Rules of Civil Procedure allow a party to request the production of documents or "other data compilations from which information can be obtained, translated, if necessary, by respondent through detection devices into reasonably usable form."[5] Moreover, courts are recognizing the enormous implication computers are having on litigation.[6]

Second, electronic data is created each time a computer is used, including information found within databases, operating systems, hard drives, floppy drives, magnetic tapes, e-mails, voice mail messages, and websites.[7]

Third, electronic data is difficult to destroy.[8] A computer user who deletes files and e-mail messages is not actually erasing the data from the computer system.[9] The computer merely marks the file as space that can be overwritten if needed, and if the space is

1. Peter Lacouture, *Discovery and the Use of Computer-Based Information in Litigation*, 45 RHODE ISLAND B. J. 9, 9 (1996).

2. Jeff Lendino, *Buried in the Bytes the Coming of Age of Electronic Discovery*, 17 LAW. PC 6, July 15, 2000.

3. Lacouture, *supra* note 1, at n.1.

4. Recently, a South Dakota Internet company, BrightPlanet.com, released a report claiming the discovery of the "deep Web," which BrightPlanet.com defines as "a vast reservoir of Internet content that is 500 times larger than the known 'surface' World Wide Web." Michael K. Bergman, *The Deep Web: Surfacing Hidden Value*, (July 2000), *at* http://www.completeplanet.com. The report alleges that the "deep Web" contains nearly 550 billion individual documents, compared to the one billion contained in the "surface Web." *Id.*

5. FED. R. CIV. P. 34(a); MINN. R. CIV. P. 34.01.

6. *E.g.*, Bills v. Kennecott Corp., 108 F.R.D. 459, 462 (D. Utah 1985) (stating that "[c]omputers have become so commonplace that most court battles now involve discovery of computer-stored information"); MANUAL FOR COMPLEX LITIGATION (Third) § 21.446 (1995).

7. Christine Sgarlata Chung & David J. Byer, *The Electronic Paper Trail: Evidentiary Obstacles to Discovery and Admission of Electronic Evidence*, 4 B.U. J. SCI. & TECH. L. 5, 8 (1998).

8. *Id.* at 12.

9. *Id.*

never overwritten, that data can exist in the exact form as when it was created, unbeknownst to the user.[10]

Fourth, electronic data will often contain information that would not exist in paper form, especially in e-mail messages.[11] Many "smoking guns" have been found in e-mail messages because of the informally unique nature of e-mail.[12] E-mail users tend to believe that because of the easy access to the delete key, they can exercise less discretion in their choice of words by using inappropriate, "off-the-cuff language" that would not be used in normal conversation or correspondence.[13]

This paper will focus on the issues practitioners can expect to encounter when litigation involves electronic data, both as the subject matter of a dispute, and as trial evidence. The paper will also discuss issues practitioners should be aware of when counseling clients about managing electronic information.

Part II will attempt to familiarize practitioners with the world of electronic data by describing the terms and sources of electronic data one can expect to encounter. Part III will discuss how courts have responded to electronic data discovery issues. Part IV explains how practitioners can obtain and use electronic data, and how to defend against requests for electronic data.

Finally, Part V offers suggestions for counseling clients about spoliation of evidence issues, as well as the issues clients must deal with to effectively use and manage electronic data via the Internet and e-mail.

II. WHERE TO FIND ELECTRONIC DATA

To properly handle electronic data discovery, practitioners must familiarize themselves with the terminology and the available technology.[14] Understanding the technology and terminology will give practitioners an idea of where to look for electronic data, and allow for accurate discovery requests capable of withstanding an

10. *Id*; James H. A. Pooley & David M. Shaw, *Finding Out What's There: Technical and Legal Aspects of Discovery*, 4 TEX. INTELL. PROP. L.J. 57, 60 (1995); Andrew Johnson-Laird, *Smoking Guns and Spinning Disks*, 11 COMPUTER LAW 1, 2 (1994).

11. Chung & Byer, *supra* note 7, at 19.

12. Joshua M. Masur, *Safety in Numbers: Revisiting the Risk to Client Confidences and Attorney-Client Privilege Posted by Internet Electronic Mail*, 14 BERKLEY TECH. L.J. 1117, 1131 (1999).

13. *Id.*

14. Pooley & Shaw, *supra* note 10, at 61.

"unduly burdensome" objection.[15] Electronic data falls into three general categories: data files, electronic mail, and background information.[16]

A. *Data Files*

Data files consist of four general types of information that is processed and stored electronically: active data, archival data, backup data, and residual data.[17] Active data is readily accessible, and comes in many formats, such as word processing documents, spreadsheets, databases, e-mail messages, and electronic calendars.[18] Active data files are accessed through programs such as File Manager and Explorer in the Microsoft Windows environment.[19]

Archival data is stored separately from active data because it is no longer in use.[20] Some computer systems have automatic backup systems, which create backup data files, or "file clones," while the user is creating a document.[21] These "file clones" are then used to assist the user in recreating the file should a malfunction occur.[22] Backup data files are a beneficial place to look for evidence as many versions of a particular document may exist in this format.[23]

Backup data provides access to information in the event of a malfunction because the data has been copied to a storage medium, such as floppy disks, magnetic tapes, zip drives and CD-ROM.[24] Backup data is a good source of historical information, as many businesses routinely use backup procedures which can hold data going back years.[25] The downside to the discovery of backup data results from the ability of backup storage media to hold incredibly large amounts of data. If the backup data filing system is poorly organized, much time and expense is required to sort

15. *Id.*
16. Joan E. Feldman & Rodger I. Kohn, *The Essentials of Computer Discovery*, 1998, *available at* WESTLAW, LW GLASS-CLE 297; Carey Sirota Meyer & Kari L. Wraspir, *E-Discovery: Preparing Clients for (and Protecting Them Against) Discovery in the Electronic Information Age*, 26 WM. MITCHELL L. REV. 939, 945-50 (2000).
17. Feldman & Kohn, *supra* note 16, at 300-01.
18. *Id.* at 300.
19. *Id.*
20. *Id.*
21. *Id.*
22. *Id.*
23. *Id.*
24. *Id.* at 301.
25. *Id.*

through the information.[26]

Residual data still exists on disk drives and in the memory of printers and fax machines, even though users "deleted" the files.[27] Files that are "deleted" are merely marked as available space, and the information will remain intact until other data or programs overwrite the space.[28] Even if new files or programs use the space containing the "deleted" information, some of the "deleted" information will remain intact if the new file or program is smaller in size than the "deleted" file.[29]

B. Electronic-mail

The second category of electronic evidence is electronic mail. The characteristics of e-mail combined with the number of e-mail messages traveling the data wires of businesses and households make it an excellent source for evidence.[30] E-mail is difficult to erase not only because of the difficulty in truly "deleting" data, but also because of the reply and forwarding features of most e-mail systems that can send an e-mail message to a virtually unlimited number of users.[31] Moreover, users of e-mail will occasionally rely on the fallacy that e-mail messages are easily destroyed, and therefore "express frank thoughts and opinions that they would not put in a formal memorandum or letter."[32]

C. Background Information

The final category of potential electronic evidence is the background information a computer system can create, such as audit trails, access control links, and non-printing information.[33] Audit trails contain information about who accessed a computer, when access occurred and for how long, what information was accessed, and whether any modifications were made to the accessed information, including the downloading of accessed information.[34]

---

26. *Id.*
27. *Id.* at 302.
28. *Id.*
29. *Id.*
30. *Id.*
31. *Id.* at 303.
32. *Id.*
33. *Id.*
34. *Id.*

Access control lists are used to limit employee access to a company's computer systems in such a way that the lists can describe who has access to particular information, thus allowing for increased ability to establish ownership or authenticity of the information.[35]

Finally, non-printing information is data that exists as part of a file or document, but does not print on the document.[36] Non-printing information can include a "time stamp" that will indicate when a document was created, modified, or deleted. In addition, non-printing data can contain notes or comments that users place in their documents when created with a program that allows a user to insert "hidden" comments in the text.[37] The "hidden" comments do not become part of the printed version.[38]

Understanding how computers store information, and where to look for information, is vital for successful discovery in litigation involving electronic data. Likewise, understanding how courts have responded to electronic data discovery disputes can assist in successful electronic discovery ventures.

III. THE JUDICIAL RESPONSE TO ELECTRONIC DATA DISCOVERY

While procedural rules allow for the discovery of electronic information, predicting the outcome of computer-related discovery matters is difficult in light of the benefits and burdens of electronic data discovery. Even before the 1993 amendment to Rule 26 requiring pretrial disclosures, courts faced discovery requests for computerized materials testifying witnesses relied upon. When dealing with the discovery of information concerning trial testimony, courts will consider the need to prepare for effective cross-examination, especially when dealing with expert testimony.[39] In *City of Cleveland v. Cleveland Electric Illuminating Co.*,[40] the court granted defendant's motion to compel production of the data and calculations that formed the basis of the plaintiff's expert's conclu-

35. *Id.* at 304.
36. *Id.*
37. *Id.*
38. *Id.*
39. Mark D. Robins, *Computers and the Discovery of Evidence – A New Dimension to Civil Procedure*, 17 J. MARSHALL J. COMPUTER & INFO. L. 411, 428 (1999).
40. 538 F. Supp. 1257 (N.D. Ohio 1980).

sions.[41] The court concluded that discovery of complex data and calculations relied upon by an expert, which are not disclosed within the expert's reports, is essential for effective cross-examination.[42] The court reasoned that cross-examination of a witness whose opinions are based on computerized data becomes impaired because of "the difficulty of knowing the precise methods employed in programming the computer as well as the inability to determine the effectiveness of the persons responsible for feeding data into the computer."[43]

In the context of discovering computerized information for trial testimony preparation, courts are usually liberal in allowing access to various materials, as long as the materials are necessary for effective cross-examination.[44] In *Fauteck v. Montgomery Ward & Co.*,[45] the court ordered the defendant to produce a database created to serve as foundation for expert testimony. The database contained the defendant's personnel records.[46] The court was not persuaded by the defendant's claim of work product, and found that production of the database was necessary for effective cross-examination.[47]

In the discrimination case of *Williams v. E.I. du Pont de Nemours & Co.*,[48] the court compelled the plaintiff to produce not only the database the plaintiff's expert compiled, but also all codebooks, user manuals, and any other documents relied upon in creating and using the database.[49] Again, the court felt disclosure was necessary for effective cross-examination.[50]

In the products liability case of *Bartley v. Isuzu Motors Ltd.*,[51] the defendant sought disclosure of computerized accident simulations conducted by the plaintiff's expert.[52] The defendant wanted not only the simulation to be used at trial, but all simulations the expert ran before deciding which simulation to use at trial as well.[53]

41. *Id.* at 1267.
42. *Id.*
43. *Id.* at 1266.
44. Robins, *supra* note 39, at 430.
45. 91 F.R.D. 393 (N.D. Ill. 1980).
46. *Id.* at 398.
47. *Id.*
48. 119 F.R.D. 648 (W.D. Ky. 1987).
49. *Id.* at 651.
50. *Id.*
51. 151 F.R.D. 659 (D. Colo. 1993).
52. *Id.* at 660.
53. *Id.*

Over the plaintiff's objections, the court allowed the defendant's request, reasoning that a party cannot defend against computer-aided simulations unless the party is allowed "access to the data that represents the computer's work product ... the data [entered] into the computer, the programs used to manipulate the data and produce the conclusions, and the theory or logic employed by those who planned and executed the experiment."[54]

While Rule 26 does not mandate the disclosure of non-testifying expert opinions, certain circumstances may allow for such discovery. In *Pearl Brewing Co. v. Jos. Schlitz Brewing Co.*,[55] the plaintiff's expert testimony relied upon a computer program developed by the plaintiff's non-testifying experts.[56] Not only did the court require production of all documents concerning the details of the computer program, the court allowed the defendant to depose the non-testifying expert for further information about the computer programs.[57] The court justified the deposition because of the defendant's need to fully understand the nature of the computer programs, and the non-testifying experts were the only persons with knowledge of the computer programs.[58]

Cases decided before the 1993 Rule 26 amendments, combined with the current version of Rule 26, provide convincing authority for liberal discovery into computerized materials relied upon by witnesses, especially expert witnesses, and in some cases, non-expert witnesses. Not only is effective cross-examination a convincing factor in broadening the scope of computerized discovery for trial testimony, failure to allow a party sufficient access could become grounds for error.[59]

A relatively more difficult line to draw for the judiciary than the discovery of computerized materials relating to trial testimony is the discovery of computerized information intended for use as evidence at trial.[60] The difficulty lies in balancing the benefits with

54. *Id.*
55. 415 F. Supp. 1122 (S.D. Tex. 1976).
56. *Id.* at 1134.
57. *Id.* at 1139.
58. *Id.* at 1138-39.
59. Shu-Tao Lin v. McDonnell Douglas Corp., 574 F. Supp. 1407, 1412-13 (S.D.N.Y. 1983) (granting a motion to set aside verdict for inadequate disclosure of computer data expert relied upon at trial), *rev'd on other grounds*, 742 F.2d 45, 47 (2d Cir. 1984).
60. Robins, *supra* note 39, at 434.

the burdens, such as the costs of production, business disruptions, and the disclosure of privileged information.[61] Cases where the benefits will most likely outweigh the burdens occur when computer hardware or software is the focus of the dispute, such as patent, copyright, and trademark infringement.[62]

For example, in *Playboy Enterprises, Inc. v. Welles*,[63] the plaintiff alleged trademark infringement by the defendant through use of the plaintiff's trademarks on the defendant's website.[64] The plaintiff sought production of the defendant's hard drive in an attempt to uncover deleted e-mails not produced during earlier discovery.[65] Recognizing the defendant's privacy rights and the attorney-client privilege, the court nonetheless granted the plaintiff's request for production of the defendant's hard drive.[66]

Other cases involving the use of electronic data as evidence include instances where stored electronic data is at issue.[67] For example, in *Smith v. MCI Telecomms. Corp.*,[68] the plaintiff claimed her former employer failed to pay an appropriate commission.[69] To assist with her claim, the plaintiff requested production of computer manuals the defendant objected to as irrelevant to the calculation of commissions.[70] The court ordered production, in part because the manuals were relevant to other issues in the case, including order entry, order control, order maintenance, and order installation.[71]

---

61. *Id.*
62. *Id.*
63. 60 F. Supp. 2d 1050 (S.D. Cal. 1999).
64. *Id.* at 1051.
65. *Id.* at 1052.
66. *Id.* The court protected the defendant's privacy and attorney-client privilege through use of a detailed protocol and protective order. *Id.* at 1054-55; Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 640 (S.D. Ind. 2000). In *Simon Property Group*, the plaintiff wanted to recover deleted files from the defendant, and moved the court for an order compelling the defendant to produce all home and office computers used by four of the defendant's employees. *Id.* at 640-42. The court ordered production of all computers as requested by the plaintiff, subject to a protocol that would limit any undue burden on the defendant in terms of business interruptions and privacy. *Id.* The court used the protocol outlined in *Playboy*, 60 F. Supp.2d at 1054-55, as a model to limit the undue burden. *Simon Property Group*, 194 F.R.D. at 641.
67. Robins, *supra* note 39, at 435.
68. 137 F.R.D. 25 (D. Kan. 1991).
69. *Id.* at 26.
70. *Id.*
71. *Id.* at 27.

In *Armstrong v. Bush*,[72] another case involving the storage of electronic data, the plaintiffs challenged the National Security Counsel's (NSC) guidelines for preserving computer-related information under the Federal Records Act.[73] The court granted the plaintiff's request for several types of computer-related information. For example, NSC was required to provide information on the oral training computer uses received concerning the types of communications sent and received, and how information is saved, deleted, and manipulated.[74] NSC was also ordered to provide information on NSC's practice of modifying its communications and recording computer software.[75]

Obtaining electronic data simply because computer-related information is an issue does not guarantee access through discovery. A court will, in certain circumstances, deny computerized data discovery on the basis that even though electronic records may contain more data than hard copies, the difficulty in determining the relevance of the information and the cost of production does not justify the burden of production.[76]

In the discrimination case of *Williams v. Owens-Illinois, Inc.*,[77] the court denied the plaintiff's request for production of computer tapes of the defendant's statistical database.[78] The court allowed limited disclosure by ordering the defendant to perform certain computer runs, but denied complete disclosure when the information on the tapes was available from other sources.[79]

IV. HOW TO OBTAIN AND DEFEND DISCOVERABLE ELECTRONIC DATA

In the electronic data context, procedural tools for discovery of information are often affected by technological considerations unfamiliar to some practitioners.[80] The combination of procedure and technology issues raise important strategic questions during discovery, such as timing and the cost of discovery in relation to the

72. 139 F.R.D. 547 (D.D.C. 1991).
73. *Id.* at 549-50.
74. *Id.*
75. *Id.* at 553-54.
76. Robins, *supra* note 39, at 487.
77. 665 F.2d 918 (9th Cir. 1982).
78. *Id.* at 932-33.
79. *Id.*
80. Robins, *supra* note 39, at 485.

importance of the evidence.[81]

A. *Obtaining Electronic Data*

Once litigation has commenced, an early opportunity for discovery of electronic data occurs through use of the mandatory disclosure requirements of Rule 26(a)(1)(B), which require the production of copies or a description by category of relevant documents and data compilations.[82] While mandatory disclosures may provide a good starting point for later discovery of more specific information, the disclosures are not required until ten days following the Rule 26 discovery plan meeting.[83]

Between the time of mandatory disclosures, and a party's response to additional discovery, important electronic data remains subject to deletion through ordinary use of computers.[84] Ordinary use includes simply turning the computer on or off, entering data, loading software, or performing maintenance.[85]

Once the prospect of litigation is high, and certainly no later than the initial service of process, counsel should consider placing all opposing parties on notice of the duty to preserve relevant evidence, including electronic data.[86] The importance of sending opposing parties notice is not only to place the duty to preserve the electronic data on the party, but also to prevent data destruction through the continued use of a computer.[87]

To further guard against the destruction of relevant data, the notice should outline the types of data to be preserved, including

---

81. *Id.*

82. FED. R. CIV. P. 26(a)(1)(B). According to the 1993 Advisory Committee Notes, disclosure under this rule

> should describe and categorize ... the nature and location of potentially relevant documents and records, including computerized data and other electronically-recorded information, sufficiently to enable opposing parties (1) to make an informed decision concerning which documents might need to be examined, ... and (2) to frame their document requests in a manner likely to avoid squabbles resulting from the wording of the requests.

Id. at Advisory Committee Note.

83. FED. R. CIV. P. 26(a)(1).

84. Robins, *supra* note 39, at 487.

85. Feldman & Kohn, *supra* note 16, at 306.

86. Lacouture, *supra* note 1, at 10; Feldman & Kohn, *supra* note 16, at 318-20. The authors give an example of a comprehensive "notice" letter. *Id.*

87. Pooley & Shaw, *supra* note 10, at 62.

active and backup data files.[88] The notice should explain where the information might exist, and should include a request the cancellation of document and data destruction protocols, both for hard copy and in electronic form.[89]

Counsel should also advise their opponent that users of their systems should refrain from saving files or loading software to existing drives and peripheral devices, and to discontinue compression and defragmentation protocols.[90]

In some instances, a party may want to take extraordinary procedures to guard against intentional and unintentional destruction of potential evidence. One such option is the ex parte seizure order, which can be granted and executed before a defendant is even aware of a lawsuit.[91] However, authority for an ex parte order must come from statute or rule and meet various constitutional requirements.[92]

The constitutional requirements of an ex parte order include conforming to due process requirements,[93] restricting searches and seizures,[94] and allowing free speech.[95] These types of requirements have been held to apply in civil cases.[96] Statutes and rules to consider for ex parte authority include Rule 65 of the Federal Rules of Civil Procedure,[97] the Trademark Counterfeiting Act of 1984,[98] and the Copyright Act.[99] The provisions in each of these statutes are designed to meet constitutional requirements, but proponents of ex parte orders carry a heavy burden of proof and must consider

88. Feldman & Kohn, *supra* note 16, at 306. The authors also suggest including e-mail and any non-printing information associated with e-mail messages, data files, application software such as spreadsheets and word processors, types of databases and associated structure, network logs, and electronic calendars. *Id.*

89. *Id.* at 307.

90. *Id.*

91. Robins, *supra* note 39, at 487; First Tech. Safety Sys., Inc. v. Depinet, 11 F.3d 641, 649-50 (6th Cir. 1993) (explaining standard for justifying an ex parte seizure order in misappropriation of trade secret case).

92. Robins, *supra* note 39, at 487-89.

93. U.S. CONST. amend. V; Mathews v. Eldridge, 424 U.S. 319, 332 (1976).

94. U.S. CONST. amend. IV; 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT §§ 1.7(a), 1.7(g), 2.4(b) (3d ed. 1996).

95. U.S. CONST. amend. I.

96. *E.g.*, Time Warner Entm't Co. v. Does Nos. 1-2, 876 F. Supp. 407, 411-412 (E.D.N.Y. 1994); Paramount Pictures Corp. v. Doe, 821 F. Supp. 82, 86-91 (E.D.N.Y. 1993).

97. FED. R. CIV. P. 65(b); MINN. R. CIV. P. 65.01.

98. 15 U.S.C.A. § 1116(d)(1)(A) (1997).

99. 17 U.S.C.A. § 503(a) (1995).

the consequences of moving for an order.[100]

Additional authority to consider for early access to computer-related information is found in Rule 16 of the Federal Rules of Civil Procedure.[101] Rule 16 gives the court power to issue orders designed to control the handling of discovery issues before a scheduling order is issued.[102] While proceeding for a preservation order under Rule 16 can prove helpful because of the early nature of the order, the party proceeding under the rule should acquire prior knowledge of their opponent's computer systems to assist the judge in addressing all relevant concerns.[103]

Finally, a party may seek expedited discovery under Rule 26(d), which allows a court to commence discovery earlier, [104] or Rules 33(b)(3) and 34(b), which allow the court to decrease the thirty-day period a party is allowed to respond to interrogatories and requests for inspection and production.[105]

Whether discovery is proceeding in a non-expedited fashion, or a party is faced with expedited discovery and requires information for a pretrial conference, counsel must decide whether to obtain the necessary information through interrogatories, depositions, or requests for inspection and production. Not only must the mode of discovery be appropriate, but also the substance of the discovery request must be tailored specifically enough to uncover the needed information, yet avoid relevance, vague, and unduly burdensome objections.[106]

Discovery requests should focus on obtaining information from specific sources in specific locations.[107] Counsel might consider using an expert to assist in framing discovery requests to identify potential sources of information, such as operating systems, da-

100. Robins, *supra* note 39, at 491-500. The author discusses necessary requirements of Rule 65, the Trademark Counterfeiting Act of 1984, and the Copyright Act. *Id.* at 491-496. The author also explains that by requesting such an order, a party faces a denial accompanied by a judicial opinion on the claim's merits. *Id.* at 499. If granted, the requesting party might face higher than expected costs, finding nothing of probative value, or having the order vacated in later proceedings. *Id.*

101. FED. R. CIV. P. 16(a); MINN. R. CIV. P. 16.01.

102. FED. R. CIV. P. 16(a); MINN. R. CIV. P. 16.01.

103. Robins, *supra* note 39, at 501.

104. FED. R. CIV. P. 26(d); Robins, *supra* note 39, at 502.

105. FED. R. CIV P. 33(b)(3); FED. R. CIV. P. 34(b); Robins, *supra* note 39, at 502.

106. Robins, *supra* note 39, at 505; Pooley & Shaw, *supra* note 10, at 61.

107. Robins, *supra* note 39, at 505.

tabases, networks, servers, desktop computers, laptop computers, portable computing devices, and home computers.[108] Other areas to consider when drafting discovery are storage media such as memory, hard disks, floppy disks, magnetic tapes, and CD-ROMs, whether used on a daily basis or for backup, and whether stored on-site or off-site.[109]

Whichever discovery options are chosen, counsel needs to first gain specific information on the structure of the opponent's system.[110] Specific information consists of the system's configuration, which includes the types of computers and hardware used by all personnel; the type of all network and communication systems, hardware, and software, including e-mail systems and a list of users.[111]

Counsel should request specific information on application software and utilities, including brand and version, for both commercial and custom applications.[112] Counsel will need specific information on the name and version of all backup software, procedures and frequency of backup protocols, including partial or complete system backups, the type and location of backup and storage media, the length of time backup tapes are stored and reused, and how backup data is categorized.[113]

---

108. *Id.*
109. *Id.;* Lacouture, *supra* note 1, at 9.
110. Feldman and Kohn, *supra* note 16, at 307.
111. *Id.*
112. *Id.* at 308.
113. *Id.* The authors suggest the following as a sample request for document production:

> Written policies, procedures and guidelines as they relate to computers, electronic data, and electronic media as they relate to:
> a. File naming conventions and standards
> b. Diskette labeling standards
> c. Backup tape rotation schedules
> d. Electronic media retention/destruction schedules
> e. Corporate policies concerning employee use of company computers and data.

Id. at 321-23. The authors also provide extensive definitions for document production requests. *Id.;* Lacouture, *supra* note 1, at 30-1. The author provides the following as a sample definition for document production requests:

> Document means any writing, drawing, graphic material or data compilation, including, without limiting the generality of the foregoing, agreements, contracts, notes, work papers, memoranda ... [insert additional descriptive phrases as preferred], whether stored in tangible, electronic, mechanical or electric form or representation of any kind (including (i) materials on or in computer tapes, disks and memory and (ii) backup

One commentator suggests first learning about the opponent's computer system through interrogatories, followed by depositions of the appropriate computer personnel, followed by an on-site inspection.[114] If an on-site inspection is contemplated, using a computer expert to assist with drafting interrogatories and deposition questions will greatly increase the chances of a complete and thorough inspection.[115]

Interrogatories can reveal information necessary to know where to locate evidence, the type of evidence to request production of, the structure of the organization, the identity of appropriate individuals to depose concerning computer system use and maintenance, and the procedures necessary to obtain the evidence.[116]

---

copies and "deleted" files on a computer storage device or media) whether located on-site or off-site. All drafts, copies or preliminary material which are different in any way from the executed or final document shall be considered to be additional documents as that term is used herein.

Id.

114. Robins, *supra* note 39, at 505.

115. Joseph L. Kashi, *How to Conduct On-Premises Discovery of Computer Records*, 24 LAW PRAC. MGMT. 26, 28 (Mar. 1998).

116. Lacouture, *supra* note 1, at 9. The author suggests the following as sample interrogatories:

1. Describe the computer systems(s) used by [plaintiff/defendant] currently and at any time within the past [#] years, including, but not limited to, for each such system, the brand and model of the computer, the amount of memory and size of the hard disk, the version of the operating system, the type and version of network software, if any, the brand and model of all peripheral devices including tape drives, external disk drives, other storage devices and modems; the brand and version of major software in use of the system(s) during such period, and the name of all online (electronic) services that have been accessed with the system(s) during such period.

2. Provide the name, employer, title, business and home addresses and telephone numbers for each person with operational or maintenance responsibility for the computer system(s) described above [during time period], including, but not limited to, the person(s) who maintain the hardware described in (1) above, the person(s) responsible for installing new and upgraded software on the system(s), the person(s) responsible for the day-to-day operation of the system(s), and the person(s) responsible for making backups or archiving files and data on the system(s).

3. Describe policies and procedures followed by [plaintiff/defendant] for backing up files and data on the computer system(s) described in (1) above, including, but not limited to, the frequency of backups, the type of backup (full, differential or incremental), the software used during [period], the number of sets of tapes or other media and the rotation of

Depositions can yield additional information on the organization's methods for use of hard copy versus electronic copy, file and e-mail deletion policies, and other forms of storage.[117] Rule 30(b)(6)[118] depositions of the opponent's information systems department head can reveal information about the opponent's computer system necessary for further discovery, and can assist in establishing foundation for use of the electronic data as evidence.[119]

---

such media, and whether such policies are in writing.

4. Describe all record retention and destruction policies and procedures followed by [plaintiff/defendant] during [period] including, but not limited to, the date the policy was adopted, the types of documents covered and the respective retention periods, the frequency of document destructions, whether any record is kept of what documents are destroyed, the manner the policy is communicated to [plaintiff's/defendant's] employees, and the identity of all employees with responsibility for implementing and executing the policy.

Id. at 31.

117. Robins, *supra* note 39, at 506.

118. FED. R. CIV. P. 30(b)(6).

119. Feldman & Kohn, *supra* note 16, at 308. The authors suggest the following as sample deposition questions:

System Profile

1. Describe the types of computer system(s) used by your company in the course of business.

2. Describe/identify the type of software used on your computer system(s).

3. Identify the person(s) responsible for the ongoing operation, maintenance, expansion, backup and upkeep of the computer system.

4. Does the staff [or inquire after key witnesses] have home computers used for business purposes? (If yes, repeat questions 1-2).

5. Are passwords or encrypted files used on any of the computer systems? If yes:

5.1 Describe how files are protected.

5.2 Who could provide access codes if required?

6. Have you modified your use of computers to comply with recent discovery requests?

Backup and Retention

7. List all computer systems in the organization that are backed up.

7.1 Describe the backup program(s) used. (Ex: ARCserve, StorageExpress, Maynard, Tecmar, etc.)

7.2 Give details of your backup procedures.

8. Have you modified your backup procedures to comply with recent discovery requests?

9. Are files ever deleted from the computer system(s)?

10. Are archival backups ever created? If yes:

10.1 What files have been archived?

10.2 Where are the archival backups maintained?

11. Describe any disaster recovery plans in place now and for the relevant time period.

Once the initial interrogatories and depositions reveal enough technical information to understand the opponent's computer systems, an on-site inspection of the opponent's computer system can generate additional electronic evidence.[120] To perform the actual inspection, one commentator suggests using a neutral expert without any conflicts of interest, and who is willing to sign a nondisclosure agreement.[121] To avoid claims of damaged data or evidence spoliation, the expert should allow the employees of the opponent

---

Maintenance and Access
12. Are utility programs used on computer(s) in the office? (Ex: Norton Utilities, MacTools, network maintenance programs) If yes:
12.1 Which program(s)?
12.2 Has the program been used to permanently "wipe" files? (When?)
12.3 Has the program been used to de-fragment, optimize or compress drives? (When?)
13. How do those outside of the company access the computers?
14. How are office computers secured?
15. Have any computer hardware been upgraded in the past 12 months?
16. Has any computer software been upgraded or replaced on office computers in the past 12 months?
Chain of Custody/Authentication
17. Are individual directories purged when an employee leaves the company?
18. Are passwords and access codes revoked when an employee leaves the company?
19. Are workstations reassigned to incoming employees? If yes:
19.1 Are hard drives wiped or re-formatted for the new user?
19.2 Are hard drives backed up before the new user takes system?
20. Describe how used or replaced equipment is disposed of or sold.
21. Describe how used disks or drives are treated before destruction or sale. (Degaussed? Shredded?)
22. Have you used outside contractors to upgrade either hardware or software? (If so, please identify)
23. Are changes or modifications made to software recorded? (Electronically? Are hard copy logs kept?)

Id. at 328-29.

120. FED. R. CIV. P. 34(a); Lacouture, *supra* note 1, at 31-32. The author suggests the following as a sample request for inspection:

> Plaintiff requests that defendant permit plaintiff to enter defendant's premises at [address] and to inspect, test, sample and copy the data, records and files (including e-mail sent or received by defendant and files located on remote computer systems that may be accessed by defendant's computer system(s)) on the hard drive(s), other storage devices, backup tapes and in memory of the following computer system(s) and any other computer systems located on said premises. [List computer systems].

Id.

121. Kashi, *supra* note 115, at 28.

to perform the necessary steps to access the system.[122] The expert should direct the employees to perform the necessary procedure for searching and copying data.[123] Depending on the circumstances, the expert should instruct the employees to perform searches using the opponent's software programs; recreate files with an undelete program; restore and examine all versions of a file; and run specialized search utilities that can locate a specific string of text anywhere on the computer system.[124] Once the information is obtained, the expert should take the necessary steps to preserve and protect the data, and maintain an appropriate chain of custody.[125]

During the discovery process, counsel should take all necessary steps to preserve the chain of custody to minimize claims of data alteration or tampering during both the copying and recovery process, and the data analysis process.[126] One commentator identifies several key elements to establishing an authentic chain of custody: refrain from adding or harming information, make a complete copy of requested data, use a reliable copy process, and use reliable security measures.[127] Use of a forensic expert to assist in assuring chain of custody and authentication is highly recommended.[128]

---

122. *Id.*
123. *Id.*
124. *Id.* at 30.
125. *Id.*
126. *Id.*
127. Feldman and Kohn, *supra* note 16, at 308-09. Specifically, the authors suggests that to prevent adding data or harming data, the target computer, as well as any devices intended to extract data, should be checked for, and protected from, viruses. *Id.* at 308. Further, original data and documents should be write-protected before copying. *Id.* To assure the making of a complete copy, a "mirror image" should be made, which will capture hidden data and residual data, as opposed to making a file-by-file copy, which may only reveal printable portions of the data or document. *Id.* To assure a reliable copying process, a method should be used that meets industry standards for reliability, is capable of independent verification, and can create tamperproof copies. *Id.* at 309. To ensure security, all copies and originals should be write-protected, properly labeled by time, date and source, and securely stored. *Id.* When analyzed, the data should be on a working copy made from the original. *Id.*
128. Kashi, *supra* note 115, at 28.

B. *Defending Requests for Electronic Data*

1. *Relevance*

When representing a party faced with a request for electronic information, it is important to understand the various grounds upon which to base successful objections. One such objection is relevance.[129] While relevance in the discovery context is broader than in the evidentiary context, a discovery request must be relevant to the subject matter.[130] For example, requesting production of an entire file cabinet where the cabinet itself is not part of the subject matter is grounds for a relevance objection, even though some files within the cabinet contain relevant information.[131]

Likewise, a relevance objection is proper when a request asks for an entire computer hard drive, or similar component, when the hard drive itself is not part of the dispute's subject matter, contains irrelevant information, and the request could be stated in terms of specific categories of information.[132]

2. *Unduly Burdensome*

A second possible objection is that compliance is burdensome or oppressive.[133] However, there is no presumption that a court will grant protection simply because responding is burdensome.[134] The proffered burden must be "undue."[135]

---

129. Hart & Plum, *Your Opponent's Electronic Medical: Some "Disk-covery" Disputes for the 21st Century*, ALI-ABA CONTINUING LEGAL EDUC., Dec. 9, 1999, *at* WESTLAW, SE63 ALI-ABA 437.

130. *Id.* at 446.

131. *In re* Horowitz, 482 F.2d 72, 74-79 (2d Cir. 1973), *cert. denied*, 414 U.S. 867 (1973).

132. *E.g., In re* Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993, 846 F. Supp. 11 (S.D.N.Y. 1994).

133. Hart & Plum, *supra* note 129, at 446; Meyer & Wraspir, *supra* note 16, at 951.

134. Robins, *supra* note 39, at 458.

135. FED. R. CIV. P. 26(b); *see generally* Kozlowski v. Sears, Roebuck & Co., 73 F.R.D. 73 (D. Mass. 1976). In *Kozlowski* the personal injury plaintiff sought production from the defendant of all complaints it received concerning burn injuries caused by the pajamas it distributed. 73 F.R.D. at 74. The defendant objected on grounds that its indexing system made it impossible to locate the requested documents. *Id.* at 75. In rejecting the defendant's argument, the court stated that compliance with Rule 34 is not excusable when a record-keeping system:

> conceals rather than discloses relevant records, or makes it unduly difficult to identify or locate them, thus rendering the production ... burden-

Moreover, inconvenience and expense, standing alone, will not suffice for protection from discovery. For example, in *Linnen v. A.H. Robins Co.*,[136] the plaintiff sought production of the defendant's back-up tapes.[137] The defendant objected on grounds that restoring and searching through the back-up tapes would be extremely expensive.[138] Recognizing the costs associated with production, the court nonetheless rejected defendant's argument, stating:

> [T]his is one of the risks taken on by companies which have made the decision to avail themselves of the computer technology now available to the business world. To permit a corporation such as [defendant] to reap the business benefits of such technology and simultaneously use that technology as a shield in litigation would lead to ... unfair results.[139]

When faced with a burdensome objection, courts consider whether "the burden or expense of the proposed discovery outweighs its likely benefits, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake ... and the importance of the proposed discovery in resolving the issues."[140] In the context of electronic data or electronic media, courts will also consider how production is going to be accomplished when weighing the burden or expense of proposed discovery with its likely benefit.

For example, in *Fennell v. First Step Designs, Ltd.*,[141] the plaintiff requested additional discovery of the defendant's computer files under Federal Rule of Civil Procedure 56(f) in the hope of finding evidence that a memo concerning the defendant's decision to terminate the plaintiff was fabricated.[142] Before entering its order denying plaintiff's request, the district court allowed the plaintiff, through an expert's affidavit, an opportunity to provide computer-

---

> some and costly .... To allow a defendant whose business generates massive records to frustrate discovery by creating an inadequate filing system, and then claiming undue burden, would defeat the purposes of ... discovery ....

Id. at 76.

136. No. 97-2307, 1999 WL 462015, at *1 (Mass. June 16, 1999).
137. *Id.* at *6.
138. *Id.*
139. *Id.* (citation omitted).
140. FED. R. CIV. P. 26(b)(2)(iii).
141. 83 F.3d 526 (1st Cir. 1996).
142. *Id.* at 530.

based evidence that the memo was fabricated.[143] After reviewing the word processing file, plaintiff's expert opined that the file was "autodated" before the date printed on the memo.[144] The court, however, failed to hold that the expert's opinion was probative of fabrication.[145] The expert also opined that the true creation date of the termination memo could be determined by reviewing the defendant's hard drive.[146]

The defendant's computer expert did not believe such a date could be determined.[147] The court held a conference and directed each party to submit a protocol for accessing the defendant's computer.[148] The court warned that discovery of the computer hard drive would only occur if the protocol assured adequate confidentiality, and a "minimal degree of intrusion time-wise and interference-wise" with the defendant's business.[149]

After reviewing each party's protocol, the court determined that the defendant's proposal was "extremely cumbersome and expensive."[150] The court also held that plaintiff's proposal failed to accurately describe the methodology of obtaining the data, and failed to protect against the disclosure or destruction of trade secrets and privileged information.[151] These factors, combined with the increase in attorney fees and costs that would arise in resolving the discovery dispute and actually obtaining the data, did not persuade the court that the benefits outweighed the costs and risks of discovery.[152]

In situations where relevance or undue burden objections are not appropriate, claims of privilege or work product might prove successful.[153]

143. *Id.*
144. *Id.*
145. *Id.* at 531.
146. *Id.*
147. *Id.*
148. *Id.*
149. *Id.*
150. *Id.* at 532, n.6.
151. *Id.* at 532-33; *see id.* at 532, n.5.(describing the plaintiff's protocol).
152. *Id.* at 532-33.
153. FED. R. CIV. P. 26(b)(1), 26(b)(3), 26(c); MINN. R. CIV. P. 26.02(a), 26.02(c), 26.03.

3. *Privilege*

A common claim of privilege involves attorney-client communications.[154] In *IBM Corp. v. Comdisco, Inc.*,[155] the defendant brought a motion to compel the plaintiff to produce an e-mail communication.[156] The e-mail communication was from a business manager to an account representative concerning legal advice the business manager received.[157] The court concluded that portions of the communication, even though transmitted by a non-attorney, were privileged because the persons involved with the communication were within "the circle of confidentiality."[158] A different "portion of the communication ... was intended to be disclosed to persons outside the circle of confidentiality," and was found not privileged.[159]

4. *Work Product*

The work product privilege is used to protect an attorney's mental impressions, opinions, and legal conclusions prepared in anticipation of litigation.[160] The privilege is designed to prevent

154. Another privilege to consider is the doctor/patient privilege. For example, in Strasser v. Yalamachi, 669 So. 2d 1142 (Fla. App. 1996), the plaintiff requested an inspection of the defendant's computer system to search for information the defendant, a surgeon, claimed was purged. *Id.* at 1144. Recognizing that the plaintiff's request was within the civil discovery rules, the court nonetheless denied the inspection because the defendant stored confidential patient information on the system, and unfettered access would cause irreparable harm. *Id.* at 1145. The court also denied the request on expert testimony that the likelihood of retrieving the information was extremely low. *Id.*

155. No. 91-C-07-199, 1992 WL 52143, at *1 (Del. Super. Ct. March 11, 1992).

156. *Id.* at *1.

157. *Id.*

158. *Id.* at *1-2.

159. *Id.* at *1.

160. FED. R. CIV. P. 26(b)(3), which reads in pertinent part:

> [A] party may obtain discovery of documents and tangible things otherwise discoverable ... and prepared in anticipation of litigation or for trial by or for another party or by or for that other party's representative ... only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of the party's case and that the party is unable without undue hardship to obtain the substantial equivalent of the materials by other means. In ordering discovery of such materials when the required showing has been made, the court shall protect against disclosure of the mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of a party concerning the litigation.

Id.; MINN. R. CIV. P. 26.02(c).

"unwarranted inquiries into the files and mental impressions of an attorney."[161] Moreover, the doctrine recognizes the necessity for an attorney to work "with a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel."[162] When deciding work product applicability, courts will consider whether the claimed work product is "ordinary work product" or "opinion work product."[163] Opinion work product will contain an attorney's mental impressions, conclusions or legal theories, while ordinary work product is all other work product, usually factual in nature.[164]

The difference between ordinary work product and opinion work product is not always clear, yet the difference is crucial in terms of the ability of the discovering parties to obtain the information. Ordinary work product is subject to disclosure if the requesting party makes a showing of substantial need, coupled with an inability to obtain the information from a different source without undue hardship.[165] On the other hand, opinion work product "enjoys a very nearly absolute immunity and can be discovered only in very rare and extra ordinary circumstances."[166]

The work product privilege plays an important role in an attorney's litigation support system, which is a computer program capable of sorting, organizing, and easily accessing information related to litigation.[167] Attorneys should consider the discoverability of litigation support systems when deciding which of the two basic

161. Hickman v. Taylor, 329 U.S. 495, 510-11 (1947).

162. *Id.*

163. Patrick R. Grady, Comment, *Discovery of Computer Stored Documents and Computer Based Litigation Support Systems: Why Give Up More Than Necessary*, 14 J. MARSHALL J. COMPUTER & INFO. L. 523, 546 (1996).

164. Upjohn Co. v. United States, 449 U.S. 383, 401 (1981); In re Murphy, 560 F.2d 326, 334 (8th Cir. 1977) (stating that Rule 26(b)(3) "establishes qualified immunity for ordinary work product that ... does not contain the mental impressions, conclusion or opinions of the attorney").

165. FED. R. CIV. P. 26(b)(3).

166. In re Murphy, 560 F.2d at 336; In re Chrysler Motors Corp. Overnight Evaluation Program Litig., 860 F.2d 844 (8th Cir. 1988). In *In re Chrysler*, a dispute arose over whether a computer tape prepared in anticipation of litigation was ordinary or opinion work product. 860 F.2d at 845-46. In deciding the tape was ordinary work product, the court held that the information was merely a "compendium of relevant evidence prepared by the attorney." *Id.* at 846 (citation omitted). In other words, the information only reflected the attorney's decision on how information was categorized, rather than an opinion, mental impression, or legal theory. *Id.*

167. Grady, *supra* note 163, at 547.

design systems to use.[168] One type of litigation support system is the full text method, which uses the full text of a document for incorporation into a database.[169] Key words are used to retrieve stored documents, and the program allows for retrieval of the actual text, does not require legal decisions, and is less expensive as support staff can handle the data entry.[170] However, the full text method may only receive ordinary work product protection.[171]

The second type of litigation support system is the index method, which uses a document summary prepared by the attorney for incorporation into a database.[172] Information in the database is then retrieved using any number of fields, such as subject matter, dates, and names of persons.[173] Since information entered into the system typically requires subjective judgments, opinion work product will usually attach.[174] However, an indexing system will usually cost more than a full-text system.[175]

If the discoverability of a litigation support system is at issue, courts will review the extent of the lawyer's involvement in the system and whether the system will be used at trial.[176] Systems created in anticipation of litigation should receive a minimum of ordinary work product immunity, subject to Rule 34 of the Federal Rules of Civil Procedure.[177] The more the system depends upon an attorney's mental impressions, opinions and conclusions, the greater the chance for immunity from disclosure.[178]

---

168. *Id.* at 549.
169. *Id.* at 547.
170. *Id.* at 547-548.
171. *Id.* at 549.
172. *Id.* at 547.
173. *Id.* at n. 149.
174. *Id.* at 549.
175. *Id.* at 548.
176. *Id.* at 549.
177. *Id.* at 549-50; FED. R. CIV. P. 34; Scott Paper Co. v. Ceilcote Co., 103 F.R.D. 591, 594 (D. Me. 1984) (finding post-accident investigative reports were not prepared in anticipation of litigation even though litigation was likely; rather, the reports were prepared in normal course of business).
178. Grady, *supra* note 163, at 549-50; Parry v. Highlight Indus., Inc., 125 F.R.D. 449, 452-453 (W.D. Mich. 1989) (holding that minimal factual content in documents does not outweigh interest in protecting attorney's mental impressions); Am. Floral Servs., Inc. v. Florists Transworld Delivery Assoc., 107 F.R.D. 258, 261 (N.D. Ill. 1985) (holding disclosure of documents would reveal attorney's decision as to the importance of documents in the case); Shelton v. Am. Motors Corp., 805 F.2d 1323, 1329 (8th Cir. 1986) (stating that attorney's decision as to the selection of documents is protected work product as the selection decision re-

Attorneys should remain constantly aware that work product privileges are not waived. Moreover, attorneys should be aware that unlike the attorney-client privilege, an inadvertent disclosure of work product could act as a waiver.[179]

Work product waiver differs from attorney-client privilege waiver in two respects. First, the policy behind work product immunity is to enhance the adversarial system, such that disclosure of a document to an opposing party is not incompatible with the policy behind work product doctrine.[180] Second, with work product, the attorney holds the privilege, and has an affirmative duty to protect documents considered work product.[181] On the other hand, with the attorney-client privilege, the client holds the privilege.[182] If an inadvertent disclosure by an attorney worked as a waiver of the attorney-client privilege, the effect "would chill clients' trust in the confidentiality of their communications, thus, undermining confi-

---

flects thought process). *But see* In re San Juan Dupont Plaza Hotel Fire Litig., 859 F.2d 1007, 1018 (1st Cir. 1988) (stating that document selection process alone is insufficient to protect documents in opinion work product); In re Shell Oil Refinery, 125 F.R.D. 132, 134 (E.D. La. 1989) (stating that attorney's theory of case would not likely be disclosed based on which documents were selected for photocopying); Bohannon v. Honda Motor Co., 127 F.R.D. 536, 539 (D. Kan. 1989) (stating that the revealing of documents will not in and of itself reveal attorney's opinions).

179. Data Gen. Corp. v. Grumman Sys. Support Corp., 139 F.R.D. 556, 561 (D. Mass. 1991) (finding the inadvertent disclosure of work product constitutes a waiver); IBM Corp. v. Comdisco, Inc., No. 91-C-07-199, 1992 WL 149502, at *1 (Del. Super. Ct. June 22, 1992) (holding inadvertent disclosure did not waive attorney-client privilege). *But see* United States v. Gulf Oil Corp., 760 F.2d 292, 295 (Temp. Emer. Ct. App. 1985) (declaring an unintentional disclosure may waive work product and attorney-client privileges).

180. *Data Gen. Corp.*, 139 F.R.D. at 558.

181. Prudential Ins. Co. v. Turner & Newall, 137 F.R.D. 178, 182 (D. Mass. 1991); *see generally* In re Chrysler Motors Corp. Overnight Evaluation Program Litig., 860 F.2d 844 (8th Cir. 1988). In *In re Chrysler*, Chrysler Motors Corp. attempted to claim work product privilege for computer tapes it prepared in anticipation of litigation, which it disclosed to the opposing party during settlement negotiations. 860 F.2d at 845. Before Chrysler disclosed the tapes, the opposing party agreed the tapes were work product, and not to be released to any other party. *Id.* The court, after finding the tapes to be work product, nonetheless ordered disclosure on the basis that Chrysler waived its privilege by merely disclosing the tapes to a third party, irrespective of a contrary agreement. *Id.* at 846-47. The court reasoned that confidentiality is the dispositive factor. *Id.* at 847. Further, even though the parties shared a common interest in settling their dispute, their agreement not to disclose did not change the fact that the tapes were not kept confidential. *Id.*

182. *Data Gen. Corp.*, 139 F.R.D. at 559.

dence in the legal system."[183]

C. *Evidentiary Issues*

For practitioners unfamiliar with the discovery of electronic data, issues concerning how the evidence is actually going to be introduced at trial should be addressed before discovery.[184] Federal and state rules of evidence will determine the admissibility of electronic data.[185] At a minimum, evidentiary rules require sufficient accuracy, trustworthiness, and reliability in the evidence before admissibility.[186]

One of the first issues confronting the admissibility of evidence is authentication.[187] Rule 901 requires a showing that "the matter in question is what its proponent claims."[188] In terms of computer-related materials, evidence is adequately authenticated if there is a showing that "the process or system produces an accurate result."[189]

Another issue to anticipate with computer-related evidence is the best evidence rule, which prefers original documents as opposed to duplicates.[190] The concern with computer-related evidence is that printouts and data stored within a computer are often copies of information obtained from another source.[191] Computer-related documents can qualify as an original, however, if the information is shown to accurately reflect the data.[192] In most instances, computerized data in duplicate form is admissible unless there is a genuine issue as to the authenticity of the original, or under the circumstances, admitting the duplicate in lieu of the original would prove unfair.[193]

---

183. *Id.*; Helman v. Murry's Steaks, 728 F. Supp. 1099, 1104 (D. Del. 1990) ("The holder of the privilege is the client. It would fly in the face of the essential purpose of the attorney-client privilege to allow a truly inadvertent disclosure ... to waive the client's privilege").

184. Pooley & Shaw, *supra* note 10, at 69.

185. Chung & Byer, *supra* note 7, at 35.

186. Robins, *supra* note 39, at 507; Pooley & Shaw, *supra* note 10, at 69.

187. Robins, *supra* note 39, at 507.

188. FED. R. EVID. 901.

189. FED. R. EVID. 901(b)(9); First Nat'l Bank of Jefferson Parish v. M/V Lightning Power, 851 F.2d 1543, 1548 (5th Cir. 1988) (holding computer printout of wage-related data not self-authenticating).

190. FED. R. EVID. 1002.

191. Robins, *supra* note 39, at 508.

192. FED. R. EVID 1001(3).

193. FED. R. EVID 1003.

Since computerized documents are out-of-court statements, the admissibility of computer-related evidence is also subject to a hearsay objection.[194] However, computerized evidence is often considered an admission by a party opponent, and therefore not subject to the hearsay rule.[195] On the other hand, if the computerized data was prepared by, or obtained from, a third party, the proponent of the evidence is required to satisfy a hearsay rule exception for admissibility.[196]

In a few instances, computer-related evidence will not require foundational concerns, absent an issue of trustworthiness raised by opposing counsel.[197] For example, computer-generated demonstrative charts, graphs, and diagrams that are accurate and prove helpful in understanding issues are admissible.[198] Once a competent witness testifies to the accuracy and helpfulness of the computer-generated evidence, the evidence will be authenticated and admitted, [199] subject to Federal Rules of Evidence 403,[200] 611(a),[201] and potentially, Rule 1006.[202]

Business and public records are other examples of evidence requiring a minimal showing of foundation and authenticity.[203] Considering that today's business and government operations would likely come to a standstill without computers, the amount of computer-generated documents produced during normal operations is exponential. As long as the evidence was produced in accordance with Rule 803(6), reliability and trustworthiness is presumed.[204] Likewise, evidence prepared in accordance with Rule

194. Robins, *supra* note 39, at 508; FED. R. EVID. 802.
195. Robins, *supra* note 39, at 508; FED. R. EVID. 801(d)(2).
196. Robins, *supra* note 39, at 509; FED. R. EVID. 803.
197. Kashi, *supra* note 115, at 327.
198. *E.g.*, United States v. Williams, 657 F.2d 199, 203 (8th Cir. 1981).
199. Kashi, *supra* note 115, at 328.
200. FED. R. EVID. 403 (excluding evidence that is prejudicial, confuses the issues, misleads the jury, wastes time, or is cumulative, if that danger substantially outweighs the evidence's probative value); MINN. R. EVID. 403.
201. FED. R. EVID. 611(a) (trial court has discretion over mode and presentation of evidence); MINN. R. EVID. 611(a).
202. FED. R. EVID. 1006 (summaries, in lieu of voluminous writings, recordings or photographs, which cannot be conveniently examined in court, are admissible provided all parties receive originals or copies); MINN. R. EVID. 1006.
203. Kashi, *supra* note 115, at 328.
204. FED. R. EVID. 803(6) (records of regularly conducted activity presumed trustworthy); MINN. R. EVID. 803(6); Rosenberg v. Collins, 624 F.2d 659, 665 (5th Cir. 1980) (admitting business records prepared before litigation was foreseeable

806(8) is presumed trustworthy.[205]

Not only are accuracy and trustworthiness crucial factors in the admissibility of electronic evidence, they are likewise important to the fact finder when considering the weight to give such evidence.[206] It is therefore important for practitioners to proceed carefully in discovery matters to assure accuracy and trustworthiness in the evidence sought, as well as accuracy and trustworthiness in the evidence relied upon by opposing parties.[207]

Whether counsel is attempting to discover electronic evidence for use at trial, or to oppose its use at trial, the use of a competent computer expert can prove worthwhile.[208] Counsel should even consider the use of two experts, one with general expertise and if spoliation by the opposing party is an issue, a nationally recognized data recovery expert.[209]

V. COUNSELING CLIENTS ON THE USE AND MANAGEMENT OF ELECTRONIC DATA

As the amount of electronic data increases through e-mail messages and Internet use,[210] so does the legal liability of a business.[211] Electronic data, including e-mail messages, have given rise

---

and were sufficiently trustworthy).

205. FED. R. EVID. 803(8) (public records and reports presumed trustworthy); FED. R. EVID. 901(b)(7) (records must derive from a public office where similar items are kept); FED. R. EVID. 902(4) (certified copies are self-authenticating); MINN. R. EVID. 803(8), 901(b)(7), 902(4).

206. United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988) (stating that accuracy of computer data affects the weight of the evidence, not necessarily its admissibility, similar to other types of business records).

207. Robins, *supra* note 39, at 509.

208. *Id.* at 510; *see generally* Gates Rubber Co. v. Bando Chem. Indus., Ltd., 167 F.R.D. 90 (D. Colo. 1996). In *Gates*, the plaintiff hired a technician in an attempt to prove spoliation of evidence claim against the defendant. 167 F.R.D. at 112. Unfortunately, plaintiff's claim was severely hampered by its technician's mistakes. *Id.* First, the technician, in using a program that recovers deleted files, copied the program onto the defendant's hard drive. *Id.* Consequently, the program overwrote seven to eight percent of the information on the hard drive. *Id.* Second, the technician attempted to create a "mirror image" through a file-by-file back-up, rather than a true "mirror image." *Id.* Consequently, the technician only produced an image of the hard drive consisting only of existing non-deleted files. *Id.* A true mirror image would have copied everything on the defendant's hard drive, including the creation dates of certain files that overwrote deleted files. *Id.*

209. Kashi, *supra* note 115, at 28.

210. Bergman, *supra* note 4.

211. Jonathan J. Soll, *Managing Electronic Data Risks Through an Email Retention*

to such claims as sexual harassment,[212] racial discrimination,[213] and trademark infringement.[214]

A. *Spoliation Of Evidence*

One of the most important considerations when counseling clients is the spoliation of evidence, which under appropriate circumstances, can be a basis for harsh sanctions.[215] Spoliation of evidence occurs when a party, or potential party, negligently or intentionally destroys physical evidence that results in prejudice to an opposing party.[216]

In determining whether sanctions are appropriate in a particular case, a party facing the imposition of sanctions must have a duty to preserve documents because no litigant has the duty to keep or retain every document in its possession.[217] However, one "has a duty to preserve what he knows or reasonably should know (i) is relevant to the action, (ii) is reasonably calculated to lead to the discovery of admissible evidence, (iii) is reasonably likely to be requested during discovery, and/or (iv) is the subject of a pending discovery request."[218]

Exactly when this duty arises is not precise. One court has stated that the duty to preserve arises when "a complaint is filed."[219] In contrast, some courts, including Minnesota, have held that the duty arises when one is on notice that documents are relevant, either to pending or potential litigation.[220]

Policy, 18 ACCA DOCKET 18 (April 2000).

212. *Chevron Settles Harassment Lawsuit for $2.2 Million*, THE ASSOCIATED PRESS, Feb. 22, 1995, *at* 1995 WL 4363765.

213. *E.g.*, Owens v. Morgan Stanley & Co., Inc., No. 96 Civ. 9747 (DLC), 1997 WL 403454, at *1 (S.D.N.Y. July 17, 1997). The plaintiffs, black employees of the defendant, alleged they were denied promotions when a white employee of the defendant authored and distributed racist jokes to other employees via e-mail. *Id.*

214. *E.g.*, Playboy Enter., Inc. v. Welles, 60 F. Supp. 2d. 1050 (S.D. Cal. 1999). The plaintiff alleged that the defendant used its trademarks throughout her website without authorization. *Id.* at 1051.

215. Lacouture, *supra* note 1, at 10-11.

216. Linnen v. A.H. Robins Co., No. 97-2307 1999 WL 462015, at *11 (Mass. June 16, 1999) (citing Kippenham v. Chaulk Servs., Inc., 697 N.E.2d 527, 530 (Mass. 1998)).

217. *Id.* at *11.

218. Skeete v. McKinsey & Co., Inc., No. 91 Civ. 8093 (PKL), 1993 WL 256659, at *3 (S.D.N.Y. July 7, 1993).

219. *Id.* at *4.

220. Cappellupo v. FMC Corp., 126 F.R.D. 545, 551 (D. Minn. 1989) (stating

A court's authority for imposing sanctions is discretionary and may come from a variety of sources.[221] Rule 37 of the Federal Rules of Civil Procedure allows a court to impose sanctions upon a party who did not adequately respond to discovery requests or to orders compelling discovery.[222] In situations where Rule 37 does not apply, either because litigation has not commenced, no discovery requests or orders compelling discovery exist, or state rules are inapplicable, the court can look to state and federal rules of civil procedure,[223] statutes,[224] professional conduct rules,[225] or the inherent power of the court to manage the proceedings before it.[226]

Once a court has determined that sanctions are available, the court "[h]as a broad canvas upon which to paint in determining sanctions."[227] One such sanction is the adverse inference, or "spoliation inference."[228] When a court imposes the spoliation inference, the jury is instructed that they may "[i]nfer that the party who destroyed potentially relevant evidence did so 'out of a realization that the [evidence was] unfavorable.'"[229]

A court may consider an adverse inference jury instruction once a foundation has been established to demonstrate that the party accused of destroying evidence was on notice of the claim and the relevance of the destroyed evidence.[230]

---

that "[s]anctions are appropriately levied against a party responsible for causing prejudice when the party knew or should have known that the destroyed documents were relevant to pending or potential litigation").

221. Davis v. Am. Jet Leasing, Inc., 864 F.2d 612, 614 (8th Cir. 1988); *Capellupo*, 126 F.R.D. at 550 (stating "[i]t is axiomatic that the imposition of sanctions for destruction of documents is within the trial court's discretion").

222. FED. R. CIV. P. 37; MINN. R. CIV. P. 37.01.

223. FED. R. CIV. P. 11; MINN. R. CIV. P. 11.

224. 28 U.S.C. §1927 (1994).

225. MINN. RULES OF PROFFESSIONAL CONDUCT 3.4(a) (2000).

226. *Capellupo*, 126 F.R.D. at 551 (stating that the court can rely on its inherent powers "[t]o regulate litigation, preserve and protect the integrity of proceedings before it, and sanction parties for abusive practices").

227. *Id.*

228. Mayes v. Black & Decker, 931 F. Supp. 80, 85 (D. N.H. 1996).

229. Linnen v. A.H. Robins Co., No. 97-2307, 1999 WL 462015, at *11 (Mass. June 16, 1999) (quoting Blinzer v. Marriot Int'l, Inc., 81 F.3d 1148, 1158 (1st Cir. 1996)).

230. *Linnen*, 1999 WL 462015, at *11 (citing Nation-Wide Check Corp. v. Forest Hills Distribs., Inc., 692 F.2d 214, 218 (1st Cir. 1982)); Dillon v. Nissan Motor Co., 986 F.2d 263, 269 (8th Cir. 1993) (holding that the court's use of its inherent power was proper when it instructed the jury that it "may" infer evidence as unfavorable towards the party who destroyed the evidence, rather than "requir[ing]" that the jury make such an inference).

Another available sanction is the exclusion of evidence. The exclusion of evidence was a sanction handed down in *Dillon v. Nissan Motor Co.*[231] In *Dillon*, the plaintiff was a passenger injured while riding in a vehicle manufactured by the defendant.[232] To assist with the products liability claim, plaintiff engaged the services of a number of experts to inspect the vehicle.[233] Before the plaintiffs filed their complaint, one of their experts allowed a third party to tow away and destroy the vehicle in issue.[234]

After hearing the defendant's motion to dismiss or exclude evidence, the magistrate judge found that the plaintiffs had destroyed evidence, but not in bad faith, and recommended the exclusion of the plaintiff's expert testimony.[235] The district court affirmed, and further excluded any evidence derived thereof.[236]

Monetary sanctions are another remedy utilized by courts to rectify and deter spoliation of evidence conduct.[237] Attorney's fees and costs are frequently awarded to compensate the party subject to abuse for the additional time and expense required to seek redress, including time for investigating, researching, and preparing motions, as well as depositions.[238] The court may also order monetary sanctions to reimburse the court for its time and expense.[239]

A small number of states are recognizing an independent tort

231. 986 F.2d 263, 268-69 (8th Cir. 1993).
232. *Id.* at 265.
233. *Id.* at 265-66.
234. *Id.*
235. *Id.* at 266.
236. *Id.* The district court also instructed the jury that it could infer from the destruction of the vehicle that the evidence would have been unfavorable to the plaintiffs. *Id.* On appeal, the court noted that because the plaintiff had destroyed the evidence before filing the complaint, and was therefore not subject to a discovery order, sanctions under Rule 37 of the Federal Rules of Civil Procedure did not apply. *Id.* at 267. The appellate court approved the district court's use of its inherent power to exclude the expert evidence, notwithstanding a lack of bad faith, simply because the plaintiffs knew or should have known that the car was a crucial piece of evidence. *Id.*
237. Capellupo v. FMC Corp., 126 F.R.D. 545, 552 (D. Minn. 1989).
238. *Id.*; Nat'l Ass'n of Radiation Survivors v. Turnage, 115 F.R.D. 543, 558 (N.D. Cal. 1987) (ordering defendant to reimburse plaintiff for fees and costs incurred in the discovery and preparation for the sanctions hearing, the fees and cost incurred in restoring damaged data, and fees and costs incurred as a result of the defendant's failure to produce responsive documents).
239. *Capellupo*, 126 F.R.D. at 553 (imposing $1,432.00 upon defendant for "[c]onsumption of the Court's time in hearing and considering [the] motion").

action for the intentional or negligent spoliation of evidence.[240] Although specific elements of the tort vary by jurisdiction, common elements include: (1) the existence of pending or potential litigation; (2) knowledge that litigation is pending or probable; (3) willful destruction of evidence; (4) intent to interfere with the other party's case; (5) a causal connection with the destroyed evidence and a party's inability to prove their case; and (6) damages.[241]

The most severe sanction available to the court is outright dismissal of the case, or entry of a default judgment.[242] Dismissing a case or entering a default judgment is reserved for the "most egregious offenses," but must be considered "as a last resort if no alternative remedy by way of a lesser, but equally efficient, sanction is available."[243] A party is more likely to be exposed to the severest of sanctions when the party is subject to a court order for document preservation and production, and thereafter destroys documents subject to the order.[244]

When evaluating whether a dismissal or default judgment is appropriate, a court must find that (1) the party acted willfully or in bad faith, (2) the opposing party was prejudiced, and (3) lesser sanctions would not serve the interests of punishment and deterrence.[245]

240. Steffen Nolte, *The Spoliation Tort: An Approach to Underlying Principles*, 26 ST. MARY'S L.J. 351, 353 (1995) (states recognizing a spoliation tort include Alaska, Florida, and Kansas).

241. *Id.* at 361; Foster v. Lawrence Mem'l Hosp., 809 F. Supp. 831, 836 (D. Kan. 1992) (stating the elements of the intentional spoliation of evidence tort).

242. *Capellupo*, 126 F.R.D. at 552.

243. *Id.*

244. In re Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598, 615-16 (D. N.J. 1997); Malautea v. Suzuki Motor Co., 987 F.2d 1536, 1542-43 (11th Cir. 1993) (affirming district court's decision to strike defendant's answer and enter default judgment on issue of liability for willful and bad faith violations of discovery order); Telectron, Inc. v. Overhead Door Corp., 116 F.R.D. 107, 126-28 (S.D. Fla. 1987) (entering default judgment where relevant documents were destroyed at direction of counsel on the day he was served with the complaint and a request for production of documents); St. John's Episcopal Church v. Brewmatic Co., No. C0-99-2196 (Minn. Ct. App. August 29, 2000) (entering default judgment for refusal to comply with discovery orders), *at* http://www.finance-commerce.com/court/opinions/000904/c0992196.htm. *Cf. Capellupo*, 126 F.R.D. at 553 (declining to enter default judgment where "plaintiffs have not been wholly deprived of the means to attempt their proof"); *see generally* Ins. Corp. of Ireland v. Compagnie des Bauxities de Guinea, 456 U.S. 694, 705-09 (1982) (upholding constitutionality of default judgment as discovery sanction).

245. *Telectron*, 116 F.R.D. at 130.

B. *Client Policy Considerations*

Many of the pitfalls a business faces, including spoliation of evidence, can be avoided with detailed company-wide policies covering document destruction and retention, as well as the use of e-mail and the Internet.[246]

1. *Document Retention And Storage*

While adopting a record retention policy can reduce a business's discovery burden, practitioners should consider a few important issues when advising a client about a document retention policy. First, and arguably most importantly, a proper document destruction and retention system can prevent the disclosure of unnecessary documents that could legally be destroyed.[247]

Second, the policy should be applied uniformly. If a retention policy is at issue, courts can consider "whether the record retention policy is reasonable considering the facts and circumstances surrounding the relevant documents."[248] In addition, courts may consider whether the policy was adopted in bad faith, and whether lawsuits or complaints have been filed that might suggest the retention of certain categories of documents.[249] Clients must be prepared to take all action necessary to avoid any inadvertent document destruction once the duty to preserve attaches, "as a corporation cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy."[250]

Third, the policy and software should have the capability of easy access to stored documents to ease the burden of production in terms of time and cost should litigation arise. Easy access is important since the high cost of production alone will not suffice as an objection to production. A company using available technologies will find little success in arguing that searching through and restoring large amounts of stored data or documents is unduly burdensome:

---

246. *E.g.*, Ian C. Ballon, *Spoliation of E-Mail Evidence: Proposed Intranet Policies and a Framework for Analysis*, 4 CYBERSPACE LAW. 2 (March 1999); Meyer & Wraspir, *supra* note 16, at 957-60.

247. Grady, *supra* note 163, at 533.

248. Lewy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988).

249. *Id.* (describing bad faith as adopting a retention system with the intent to limit disclosure of damaging documents); Ballon, *supra* note 246, at 2.

250. *Lewy*, 836 F.2d at 1112.

> [T]his is one of the risks taken on by companies which have made the decision to avail themselves of the computer technology now available to the business world .... To permit a corporation ... 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.[251]

Fourth, a document retention policy should further legitimize business interests, such as document storage control.[252] In addition, the policy should specify the category of files to be saved, and the period of retention for each category.[253] Consideration must also be given to all applicable government regulations concerning retention time for certain documents.[254]

Finally, a document retention policy should be flexible enough to permit necessary adjustments.[255] The policy may need to be suspended when the duty to preserve arises, when lawsuits are filed, or when new case law, statutes, or regulations change retention requirements.[256]

2. *E-Mail And Internet*

In addition to document retention, a policy governing the use of a company's e-mail system is crucial for several reasons. First, an e-mail policy containing retention and destruction guidelines will prevent the unnecessary disclosure of documents, and provide for easier access to stored e-mails during discovery.[257] Moreover, if faced with a spoliation claim for the destruction of e-mail messages, a destruction policy can become a mitigating factor.[258] Second, the company's use of an e-mail policy may decrease liability for employment-related claims.[259]

---

251. Linnen v. A.H. Robins Co., No. 97-2307, 1999 WL 462015, at *6 (Mass. June 16, 1999).

252. Lacouture, *supra* note 1, at 29.

253. *Id.*; Ballon, *supra* note 246, at 2.

254. Grady, *supra* note 163, at 533 (offering samples of record retention requirements by CFR statute title).

255. Ballon, *supra* note 246, at 2.

256. *Id.*

257. *Supra*, Part V.B.1.

258. Carlucci v. Piper Aircraft Corp., 102 F.R.D. 472, 481-82 (S.D. Fla. 1984) ("good faith disposal pursuant to a bona fide consistent and reasonable document retention policy could justify a failure to produce documents in discovery").

259. Ballon, *supra* note 246, at 2.

When advising a client on the implementation of an e-mail policy, one commentator suggests adopting an "e-mail system," rather than a "policy."[260] Using an "e-mail system" will imply the use of technology as one component of the client's overall strategy for managing electronic information, and should include an employee education component to assure proper implementation.[261] Whatever name is given to the policy, several issues need consideration.

First, e-mail should be distinguished as either official or unofficial.[262] E-mail labeled as official, or for business purposes, should be subjected to the retention policy, while unofficial e-mail, or for personal or otherwise non-business purposes, should be disposed of more frequently.[263] The policy should also consider printing hard copies, or storing electronically, all official e-mail, to lessen spoliation exposure.[264] If designating e-mail as official or unofficial is too burdensome, the client should consider separate e-mail accounts.[265]

Second, where e-mail users have access to the Internet, or outside services and networks, clients should consider restricting access to those with legitimate business needs.[266] If access to the Internet is allowed to any user, the client should consider providing several types of notices concerning appropriate subject matter and the employer's right to monitor all e-mail and Internet use. With e-mail, clients should consider having all employees sign a statement detailing the companies overall policy for e-mail use, as well as notice that the employees waive their right to privacy in e-mail, and consent to the monitoring and disclosure by the employer of all e-mail messages.[267] If having employees sign a statement proves impractical, the business can consider including a message in the computer that appears when the employee logs on to the system.[268] If an employer intends to monitor or intercept employee e-mail, the business must provide notice to employees to avoid violating the Electronic Communications Act of 1986 (EPCA).[269]

---

260. *Id.*
261. *Id.*
262. *Id.*
263. *Id.*
264. *Id.*
265. *Id.*
266. *Setting Up a Corporate Policy for Internet Use: A Checklist*, 12 COMPUTER L. STRATEGIST 4, 5 (October 1995).
267. *Id.*
268. *Id.*
269. 18 U.S.C.A. § 2510-20 (1988). The EPCA criminalizes the act of inten-

When dealing with a policy for Internet use, attorneys should remind clients that any information transmitted outside the local network becomes available to the world. To lessen the likelihood of liability-creating transmissions from either leaving the company, or entering the company through its computers, clients should consider limiting the length of messages; requiring the use of subject headings; and prohibiting the use and dissemination of abusive, offensive and obscene language and material.[270]

When drafting e-mail and Internet policies, several issues should be addressed relative to liability and discoverability. First, an understanding of the clients e-mail system is crucial. Does the system store e-mail in multiple locations, such as a desktop computer and a server?[271] Is the system capable of e-mail backup?[272] Does the system have e-mail destruction capability?[273] Does the system provide for automatic hard copy printing of certain documents?[274]

Second, consider how a retention policy best serves the client's interests in light of document retention regulations, and whether the client uses computers capable of remote connections, or business-related home computers.[275] Find out from the client how its employees use e-mail and the Internet for official purposes.[276] Is unofficial use of e-mail and the Internet currently allowed?[277]

Third, determine how employees use and manage the space on their computers.[278] Determine on average how many e-mail messages can fill disk space.[279] Determine the filing methods of e-mail users. Is mail regularly read and then deleted or printed?[280] If the mail is not regularly deleted, how do users manage the e-

---

tionally intercepting wire, oral, or electronic communication. *Id.* Two exceptions exist under the EPCA that allow an employer to monitor employee e-mails. First, one can intentionally intercept electronic communications if done in the "ordinary course of business." *Id.* Second, one can intercept electronic communications when one of the parties to the communication consents to the intrusion. *Id.*

270. *Setting Up a Corporate Policy for Internet Use: A Checklist*, *supra* note 266, at 4.
271. Soll, *supra* note 211, at 26.
272. *Id.* at 28.
273. *Id.*
274. *Id.* at 29.
275. *Id.*
276. *Id.*
277. *Id.*
278. *Id.*
279. *Id.*
280. *Id.* at 29-30.

mail?[281] Understanding each of the above will assist with risk analysis in the event the client's e-mail becomes discoverable.

After obtaining a thorough understanding of the clients e-mail system and the direction the client would like to take for a comprehensive e-mail policy, consider the appropriate method for training and educating e-mail users. Posting the policy on the client's website, in a newsletter article, or in a good old-fashioned memorandum are a few methods of maintaining awareness.[282]

VI. CONCLUSION

Federal and state rules of procedure, combined with case law, make it clear that electronic information is discoverable in litigation. As the use of technology continues to rise, as well as the complexity of technology, computer-related evidence will find its way into legal disputes of all shapes and sizes. To effectively represent clients, practitioners need to familiarize themselves with today's world of computers and remain dedicated to understanding the new technologies emerging on a daily basis. Practitioners must become familiar with the discovery tools and procedures not commonly used, and adapt those tools and procedures for use in uncommon situations. Even though the procedural framework for discovering electronic information may not change, the constantly changing world of technology and its effect on people and business will continue to push discovery into unfamiliar realms.

281. *Id.* at 29.
282. *Id.* at 32. The author provides an example of an e-mail policy. *Id.*

***