South Carolina Law Review

Volume 58 | Issue 1 Article 3

Fall 2006

Preserving the Duty to Preserve: The Increasing Vulnerability of Electronic Information

Maria P. Crist
University of Dayton School of Law

PRESERVING THE DUTY TO PRESERVE: THE INCREASING VULNERABILITY OF ELECTRONIC INFORMATION

MARIA PEREZ CRIST*

I. INTRODUCTION 8

II. THE DUTY TO PRESERVE ELECTRONIC INFORMATION 13
A. *The Duty to Preserve Evidence Generally* 17
1. *When Is the Duty to Preserve Triggered?* 17
2. *The Scope of the Duty to Preserve* 19
B. *Preservation of Electronic Information* 21
1. *The Lifeline of Digital Information* 24
2. *Hidden Data Within Digital Information* 26
3. *File Duplication in the Digital Environment* 29
4. *Accessibility of Digital Information* 30
C. *Document Retention and Destruction Policies and the Duty to Preserve Evidence* 34
1. *Retention Policies and the Management of Electronically Stored Information* 35
2. *Problems with Defining the Scope of the "Litigation Hold"* ... 36
3. *Compliance Issues During a Litigation Hold* 38

III. CONSEQUENCES FOR FAILING TO OBSERVE THE DUTY TO PRESERVE 43
A. *Determining Culpability for the Destruction of Digital Data* 45
1. *Termination of the Action with Clear Showing of Bad Faith* ... 45
2. *Conflicting Standards of Culpability for Sanction of Adverse Inference Instruction* 47
B. *Determining Relevance of Destroyed Digital Data and the Resulting Prejudice from its Destruction* 50
C. *A New Safe Harbor Under Proposed Rule 37(f)* 51

IV. PROACTIVE STEPS TO PRESERVE THE DUTY TO PRESERVE 54
A. *Preserving the Duty to Preserve with Pre-Litigation Notice* 55
B. *Preservation Efforts Under the Federal Rules of Civil Procedure* .. 56
C. *Preserving the Duty to Preserve by Moving for a Preservation Order* 58

V. CONCLUSION 63

---

*Maria Perez Crist, Professor of Lawyering Skills, Director, Legal Profession Program at the University of Dayton School of Law. J.D. University of Michigan Law School, B.A. Northwestern University.

I. INTRODUCTION

The explosive growth of electronically stored information and the unique character of electronic information challenge the time honored duty to preserve evidence. As information[1] migrates to an electronic environment, organizations are especially affected.[2] Organizations which once primarily maintained information in a paper form increasingly create and maintain their information in electronic[3] form: more than 90% of all business records are digital, and many businesses never commit those records to paper.[4] In addition to the usual types of business generated information, such as reports, spreadsheets, and other data compilations, an organization may generate new forms of communication information, such as e-

---

1. Within this Article, "information" is used in its broadest sense and includes the resources "that organizations harness to meet their operational, legal, historical and institutional needs." THE SEDONA GUIDELINES: BEST PRACTICE GUIDELINES & COMMENTARY FOR MANAGING INFORMATION & RECORDS IN THE ELECTRONIC AGE 3 (Ragan et al. eds. 2005), *available at* http://www.thesedonaconference.org/ [hereinafter SEDONA GUIDELINES]. The term encompasses all information that can be stored, regardless of the media used, and includes text, graphics, video, and audio files. *Id.* The Sedona Conference is a nonprofit legal policy research and educational organization that sponsors "Working Groups" on emerging legal issues and has been especially involved in resolving electronic discovery concerns. *Id.* at app. H. The Working Group on Best Practices for Electronic Document Retention & Production includes judges, attorneys, and experts, all with expertise in electronic discovery and document management matters. *Id.* at apps. G, H. Many federal courts rely on the *Sedona Guidelines* for guidance on electronic discovery issues. *See, e.g.*, Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 650 (D. Kan. 2005) (finding federal rules and case law provide insufficient guidance on the production of metadata, the court relied on the *Sedona Guidelines*' emerging standards for electronic document production); Zakre v. Norddeutsche Landesbank Girozentrale, No. 03 Civ. 0257(RWS), 2004 WL 764895, at *1 (S.D.N.Y. Apr. 9, 2004) (mem.) (relying on the *Sedona Guidelines*, along with the Federal Rules of Civil Procedure, to find that the defendant merely had to produce e-mails in a searchable CD-ROM format); Zubulake v. UBS Warburg LLC (*Zubulake I*), 217 F.R.D. 309, 320 n.61 (S.D.N.Y. 2003) (recognizing the *Sedona Guidelines*' distinction between different categories of electronic data).

2. While issues related to electronically stored information apply equally to individuals, the focus of this Article is on organizational electronically stored information.

3. Although this Article uses the terms "digital" and "electronic" interchangeably, the term digital is often preferred over electronic because digital encompasses all electronic media as it evolves. *See* Henry S. Noyes, *Is E-Discovery So Different That It Requires New Discovery Rules? An Analysis of Proposed Amendments to the Federal Rules of Civil Procedure*, 71 TENN. L. REV. 585, 623–25 (2004) (describing how proposed amendments changing the language of Rule 34 from "data compilations" to "electronically stored information" is too limiting).

4. Surveys on the growth of digital information confirm this trend:

> According to recent estimates published in *Law Technology News*, at least 93% of business documents are created electronically, and more than 35% of corporate communications never reach paper. The prevalence of e-mail as a primary form of corporate communication adds to the enormity of electronic documents in use today. According to estimates published in *Wired* magazine, U.S. office workers exchanged approximately 7 trillion e-mail messages in the year 2000.

ADAM I. COHEN & DAVID J. LENDER, ELECTRONIC DISCOVERY: LAW AND PRACTICE app. 1B, at 1-49 (2004); *see also* PETER LYMAN & HAL R. VARIAN, *HOW MUCH INFORMATION?* (2003), http://www.sims.berkeley.edu/how-much-info-2003/printable_report.pdf (reporting that 92% of all new information is stored on magnetic media, primarily hard disks, while only 0.01% is stored on paper).

mail, voice mail, and instant messaging.[5] When attempting to manage this overwhelming amount of digital information, an organization must decide what information it values and should therefore preserve and what information it can destroy in the interest of maintaining an efficient operating system. As a result, organizations implement document retention and destruction policies to manage electronic information.[6] When an organization is involved in litigation, however, opposing parties may value the organization's information quite differently. For example, information in e-mails may appear to lack any business need for preservation, but for an opposing party trying to establish an organizational intent, such information may be critical. As organizational concerns focus on the risks of accumulating and storing too much digital information and the need to control the growth of electronic information, information potentially relevant as evidence may be at risk. Clearly, one person's trash is another's treasure.

While improvements in technology make information storage easier and cheaper in an electronic form, the very nature of electronically stored information also makes the data easy to destroy as a result of document retention policies, changes in technology, or even mere carelessness. The dynamic nature of digital information gives it an ephemeral quality where information can quickly disappear, yet still be retrieved, albeit sometimes at great expense. These ironies of the digital medium pose problems for the duty to preserve—in establishing both the scope of the duty and when it is triggered.

A duty to preserve evidence exists when a party has notice that the evidence is relevant to litigation or when a party should know that the evidence may be relevant to future litigation.[7] The intentional destruction of evidence subject to this duty to preserve is sometimes referred to as spoliation,[8] which many state courts have recognized as a separate cause of action.[9] Although federal courts do not recognize

---

5. E-mail and instant messaging are growing causes for concern. In a recent survey, 24% of organizations reported that employee e-mail had been subpoenaed in the course of a lawsuit or regulatory investigation. AM. MGMT. ASS'N & EPOLICY INST., 2006 WORKPLACE E-MAIL, INSTANT MESSAGING, & BLOG SURVEY 1 (2006).

6. The United States Supreme Court recently noted that document retention policies are "common in business." Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005) (holding that destruction of documents pursuant to a document retention policy requires proof of conscious wrongdoing under a federal obstruction of justice statute).

7. Silvestri v. General Motors Corp., 271 F.3d 583, 591 (4th Cir. 2001) (citing Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998)); Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001) (citing Kronisch v. United States, 150 F.3d at 126).

8. For a description of the historical roots of spoliation, see Lawrence Solum & Stephen Marzen, *Truth and Uncertainty: Legal Control of the Destruction of Evidence*, 36 EMORY L.J. 1085, 1087–88 n.4 (1987) (citing, among other cases, The Pizarro, 15 U.S. (2 Wheat.) 91 (1817); Pomeroy v. Benton, 77 Mo. 64 (1882); Armory v. Delamirie, 93 Eng. Rep. 664 (K.B. 1722)).

9. Although virtually all state courts recognize that spoliation of evidence may lead to sanctions, only a minority of state courts recognize spoliation, whether intentional or negligent, as an independent basis for tort liability. *See generally* Thomas G. Fischer, Annotation, *Intentional Spoliation of Evidence, Interfering with Prospective Civil Action, as Actionable*, 70 A.L.R.4th 984, § 2.7 (1989 & Supp. 2006) (noting that only Louisiana, Florida, Indiana, Ohio, Montana, New Jersey, and West Virginia recognized the independent tort of intentional spoliation); Benjamin J. Vernia, *Negligent Spoliation of Evidence, Interfering with Prospective Civil Action, as Actionable*, 101 A.L.R.5th 613(a) (2002 & Supp. 2006) (noting that only Florida, Illinois, New Jersey, and New York recognized the independent tort of negligent spoliation).

a separate federal claim of spoliation,[10] a federal court may choose to impose sanctions pursuant to its inherent powers,[11] as well as under the Federal Rules of Civil Procedure.[12] These sanctions can include termination of the litigation through dismissal of the action, summary judgment, or default judgment;[13] monetary sanctions, including attorney fees or fines;[14] evidentiary sanctions, most commonly

10. Lombard v. MCI Telecomms. Corp., 13 F. Supp. 2d 621, 628 (N.D. Ohio 1998) (dismissing an attempt to bring an independent tort claim of spoliation based on an employer's failure to retain personnel records as required under 29 C.F.R. § 1602.14 (1991)). Federal courts analyze separate claims of spoliation under applicable state law. *See* MARGARET M. KOESEL & TRACY L. TURNBULL, SPOLIATION OF EVIDENCE: SANCTIONS AND REMEDIES FOR DESTRUCTION OF EVIDENCE IN CIVIL LITIGATION 2–3 (Daniel F. Gourash ed., ABA Publ'g 2006). The issues concerning this evolving separate spoliation tort are not the subject of this Article. *See generally* Kevin Eng, *Legal Update, Spoliation of Electronic Evidence*, 5 B.U. J. SCI. & TECH. L. 13 (1999) (noting that the tort of spoliation is in a gradual state of development); Bart S. Wilhoit, Comment, *Spoliation of Evidence: The Viability of Four Emerging Torts*, 46 UCLA L. REV. 631 (1998) (discussing the viability of tort actions for spoliation and concluding that courts should recognize liability for spoliation only in the case of intentional spoliation by a third party).

11. *See* Chambers v. NASCO, Inc., 501 U.S. 32, 43 (1991) (quoting United States v. Hudson, 11 U.S. (1 Cranch) at 34); Roadway Express, Inc. v. Piper, 447 U.S. 752, 764 (1980) (quoting United States v. Hudson, 11 U.S. (1 Cranch) at 34. *See generally* Robert J. Pushaw, Jr., *The Inherent Powers of Federal Courts and the Structural Constitution*, 86 IOWA L. REV. 735, 766–75 (2001) (reviewing the judiciary's inherent contempt powers).

12. FED. R. CIV. P. 37.

13. *See, e.g.*, Hayman v. Price Waterhouse Coopers, LLP, Nos. 5:98CV2876, 1:01CV1078, 2004 WL 3192729, at *33, *34, *36 (N.D. Ohio July 16, 2004) (recommending default judgment after significant discovery abuse); Metro. Opera Ass'n v. Local 100, Hotel Employees & Rest. Employees Int'l Union, 212 F.R.D. 178, 220, 231 (S.D.N.Y. 2003) (granting plaintiff's motion for judgment in its favor on the issue of liability as a sanction for defendant's discovery abuses), *aff'd on reconsideration*, No. 00 CIV. 3613 (LAP), 2004 WL 1943099 (S.D.N.Y. Aug. 27, 2004).

14. *See, e.g.*, Advantacare Health Partners, LP v. Access IV, No. C 03-04496 JF, 2004 U.S. Dist. LEXIS 16835, at *5–6, *31 (N.D. Cal. Aug. 17, 2004) (fining the defendants $20,000 for using a program to delete files from computers after the court had granted a temporary restraining order prohibiting the defendants from deleting files); United States v. Philip Morris USA, Inc., 327 F. Supp. 2d 21, 24, 26 (D.D.C. 2004) (mem.) (fining the company $2.75 million when eleven employees failed to preserve e-mails subject to a litigation hold); Procter & Gamble Co. v. Haugen, 179 F.R.D. 622, 632 (D. Utah 1998), *rev'd on other grounds sub nom.* Proctor & Gamble Co. v. Haugen, 222 F.3d 1262 (10th Cir. 2000) (sanctioning the plaintiff $10,000—$2,000 for each of the five employees that the plaintiff identified as having relevant information— when the plaintiff failed to search or preserve any of the e-mails of the five employees).

an adverse inference instruction to the jury;[15] or findings of contempt.[16] As courts encounter the destruction of electronically stored information that was under a duty to preserve, the most egregious cases receive serious sanctions. For example, the court issued a $2.75 million sanction against Philip Morris for the destruction of electronic records.[17] Despite the publicity such sanctions generate, numerous cases illustrate the broad range of excuses that allow the responsible party to avoid sanctions.[18]

This lack of accountability in the handling of electronic information receives further support in proposed amendments to the discovery-related Federal Rules of Civil Procedure.[19] Recently, the United States Supreme Court approved, without comment or dissent, dramatic changes and revisions to the Federal Rules of Civil Procedure concerning the discovery of electronically stored information and

---

15. *See, e.g.*, Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 113 (2d Cir. 2002) (holding that an adverse inference instruction is appropriate when there is "purposeful sluggishness" in the production of requested e-mails); DaimlerChrysler Motors v. Bill Davis Racing, Inc., No. Civ.A. 03-72265, 2005 WL 3502172, at *3 (E.D. Mich. Dec. 22, 2005) (holding that an adverse inference instruction was warranted after negligent destruction of e-mails once the complaint had been filed); Trigon Ins. Co. v. United States, 204 F.R.D. 277, 291 (E.D. Va. 2001) (finding it appropriate to draw an adverse inference when litigation consultants hired by the government destroyed documents); Linnen v. A.H. Robins Co., No. 97-2307, 1999 WL 462015, at *11 (Mass. Super. Ct. June 16, 1999) (mem.) (endorsing a jury instruction on the "spoliation inference" when defendant destroyed backup tapes requested by plaintiff).

16. *See* Landmark Legal Found. v. EPA, 272 F. Supp. 2d 70, 77–78 (D.D.C. 2003) (finding the agency committed contempt by reformatting hard drives and erasing e-mails in violation of an order enjoining the agency to maintain responsive information to a Freedom of Information Act request).

17. *See Philip Morris*, 327 F. Supp. 2d at 26.

18. *See, e.g.*, Quinby v. WestLB AG, No. 04Civ.7406(WHP)(HBP), 2005 WL 3453908, at *10 (S.D.N.Y. Dec. 15, 2005) (refusing to grant sanctions because the plaintiff's claim that the defendant delayed discovery by focusing on backup tapes when cheaper alternatives were available was "hyper-technical"); Drnek v. Variable Annuity Life Ins., No. CIV 01-242-TUC-WDB, 2004 WL 1098919, at *3 (D. Ariz. May 4, 2004) (finding sanctions not warranted although responding party implemented e-mail destruction policy after the law suit was filed because requesting party offered no evidence that defendants destroyed relevant e-mails); Wiginton v. CB Richard Ellis, Inc. (*Wiginton I*), No. 02 C 6832, 2003 WL 22439865, at *8 (N.D. Ill. Oct. 27, 2003) (denying sanctions when e-mails destroyed after the requesting party sent a notice along with the complaint asking responding party to preserve e-mails); Concord Boat Corp. v. Brunswick Corp., No. LR-C-95-781, 1997 WL 33352759, at *4–5 (E.D. Ark. Aug. 29, 1997) (denying sanctions when e-mails were destroyed and noting that requiring large companies to retain e-mails would be too burdensome).

19. A discovery conference in 1996 first addressed the unique problems associated with the discovery of electronically stored information. JUDICIAL CONFERENCE OF THE U.S., SUMMARY OF THE REPORT OF THE COMMITTEE ON RULES OF PRACTICE AND PROCEDURE app. C, at 18 (2005), *available at* http://www.uscourts.gov/rules/Reports/ST09-2005.pdf [hereinafter JUDICIAL CONFERENCE REPORT]. After extensive study and consideration, the Advisory Committee on the Federal Rules of Civil Procedure began re-examining the discovery rules and proposed amendments to Rules 16, 26, 33, 34, 37, and 45, which the Committee published for comment in August 2004. *Id.* At the three public hearings held in 2005, seventy-four witnesses testified and additional written comments were submitted. In light of the public comments, the Committee revised the proposed rule amendments and submitted them to the Standing Committee. *Id.* After approval from the Standing Committee, the Judicial Conference approved the proposed amendments on September 20, 2005. JUDICIAL CONFERENCE OF THE U.S., REPORT OF THE PROCEEDINGS OF THE JUDICIAL CONFERENCE OF THE UNITED STATES 37 (Sept. 20, 2005).

transmitted the proposed rules to Congress.[20] Specifically, new electronic discovery rules will create a new two-tiered system of discovery, shielding electronic information deemed "inaccessible" from the usual rules and standards of discovery.[21] In addition, the proposed rules create a "safe harbor" for electronically stored information destroyed pursuant to a document retention policy.[22] If adopted, and that appears likely, these amendments to the discovery rules will provide additional ways for litigants to avoid the duty to preserve.

In light of these new standards for electronic discovery, litigants must take a proactive stance in the face of potentially relevant electronically stored information. The usual course of litigation may find critical digital information long gone by the time a party specifically requests the information. Therefore, litigants must make additional efforts to safeguard potentially relevant electronic information. Courts must be willing to demand greater accountability for the maintenance of electronic information. Techniques such as preliminary injunctions, preservation orders, and early discussion in the discovery process are required to prevent the further erosion of the duty to preserve. Litigants and the courts must actively preserve the duty to preserve.

Part II of this Article will examine the duty to preserve within the context of electronically stored information. This analysis will begin with a discussion of electronic information, including the special features of different types of digital information and how courts are beginning to characterize this information. The Article will then explore the origins of the duty to preserve and how that duty is manifested within the electronic realm. Part II concludes that evolving standards for "accessible" and "inaccessible" information have an adverse impact on the scope of the duty to preserve evidence.

Part III of the Article turns to the sanctions available to courts when litigants fail to observe the duty to preserve. In addition to a discussion of the range of sanctions, Part III explores the standards courts use to determine the appropriate sanction. Differences in these standards and splits among the circuits have resulted in inconsistent standards for litigants to follow in deciding when and how they should preserve electronic information. This lack of consistency has led to a

---

20. Order Adopting Amendments to Federal Rules of Civil Procedure, 74 U.S.L.W. 2617 (2006); *see also* U.S. Supreme Court, Order Adopting Amendments to Federal Rules of Civil Procedure, April 12, 2006, http://www.supremecourtus.gov/orders/05ordersofthecourt.html (last visited Oct. 4, 2006); *see generally* Federal Rulemaking: Pending Rules Amendments, http://www.uscourts.gov/rules/newrules6.html#cv0804 (last visited Oct. 10, 2006) (publishing new rules). The proposed amendments to the discovery rules, as well as the Committee Notes to the proposed rules, are contained in Appendix C of the Judicial Conference Report of September 2005 and are separately paginated. Unless Congress enacts legislation to reject, modify, or defer the amendments, the new discovery rules will take effect on December 1, 2006. Order Adopting Amendments to Federal Rules of Civil Procedure, 74 U.S.L.W. 2617. For a detailed explanation of the rulemaking process, see James C. Duff, *Federal Rulemaking: The Rulemaking Process* (2006), http://www.uscourts.gov/rules/proceduresum.htm.

21. JUDICIAL CONFERENCE REPORT, *supra* note 19, app. C, at 45–47 (outlining the proposed amendments to Rule 26(b)(2) of the Federal Rules of Civil Procedure).

22. *Id.* at 86 (outlining the proposed amendments to Rule 37(f) of the Federal Rules of Civil Procedure).

proposed "safe harbor" from sanctions when information is destroyed pursuant to a document retention policy.[23] This Article suggests that the proposed safe harbor actually threatens the duty to preserve evidence. Part III demonstrates that despite a few landmark cases, litigants encounter significant hurdles when attempting to obtain sanctions for the destruction of evidence, and the proposed changes in the discovery rules will only reinforce these hurdles.

Part IV of this Article analyzes the proactive steps available to preserve the duty to preserve. From a simple letter notifying and reminding adverse parties of their duty to preserve to formal requests for a preservation order, this section examines the evolving standards for these strategies. Finally, this Article concludes that judicial trends narrowing the scope of the duty to preserve evidence and requiring overt bad faith before imposing sanctions, along with the proposed changes in the discovery rules, mandate action. If anticipated litigation will involve electronically stored information, litigants have a heightened obligation to take all steps necessary to preserve the duty to preserve and courts must understand their role in the protection of such fragile evidence.

II. THE DUTY TO PRESERVE ELECTRONIC INFORMATION

The duty to preserve evidence stems from a long-standing common law tradition[24] and continues to be a basic tenet within the goal of the fair adjudication of legal disputes. Three primary justifications serve as the basis of the duty to preserve: (1) statutory or regulatory requirements;[25] (2) voluntary assumption of

---

23. *Id.*

24. All circuits recognize the duty to preserve information relevant to anticipated or existing litigation. *See* Vazquez-Corales v. Sea-Land Serv., Inc., 172 F.R.D. 10, 11 (D.P.R. 1997) (citing Baliotis v. McNeil, 870 F. Supp. 1285, 1290 (M.D. Pa. 1994); Allstate Ins. Co. v. Creative Env't Corp., 28 Fed. R. Serv. 3d (West) 1352, 1358 (D.R.I 1994)); Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001) (citing Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998)); *In re* Wechsler, 121 F. Supp. 2d 404, 415 (D. Del. 2000); Silvestri v. Gen. Motors Corp., 271 F.3d 583, 591 (4th Cir. 2001) (citing *Kronisch*, 150 F.3d at 126); Williams v. Briggs Co., 62 F.3d 703, 708 (5th Cir. 1995); Beil v. Lakewood Eng'g & Mfg. Co., 15 F.3d 546, 552 (6th Cir. 1994) (citing Taylor v. Medtronics, Inc., 861 F.2d 980, 985 (6th Cir. 1988)); Cooper v. United Vaccines, Inc., 117 F. Supp. 2d 864, 874 (E.D. Wis. 2000) (citing Sentry Ins. v. Royal Ins. Co. of Am., 539 N.W.2d 911, 916 (Wis. Ct. App. 1995)); Concord Boat Corp. v. Brunswick Corp., No LR-C-95-781, 1997 WL 33352759, at *4 (E.D. Ark. Aug. 29, 1997) (citing Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 72 (S.D.N.Y. 1991)); Nat'l Ass'n of Radiation Survivors v. Turnage, 115 F.R.D. 543, 556-57 (N.D. Cal. 1987) (quoting Wm. T. Thompson Co. v. Gen. Nutrition Corp., 593 F. Supp. 1443, 1455 (C.D. Cal. 1984)); Procter & Gamble Co. v. Haugen, 179 F.R.D. 622, 631 (D. Utah 1998), *rev'd on other grounds sub nom.* Proctor & Gamble Co. v. Haugen, 222 F.3d 1262 (10th Cir. 2000) (citing *Gen. Nutrition*, 593 F. Supp. at 1455); Fla. Evergreen Foliage v. E.I. DuPont De Nemours & Co., 336 F. Supp. 2d 1239, 1272 (S.D. Fla. 2004) (citing Green Leaf Nursery v. E.I. DuPont De Nemours & Co., 341 F.3d 1292, 1308–09 (11th Cir. 2003)); Holmes v. Amerex Rent-A-Car, 180 F.3d 294, 296 (D.C. Cir. 1999).

25. Congress and federal regulatory agencies have promulgated numerous requirements mandating retention of specific documents and in some cases even impose criminal penalties for improperly destroying information subject to the requirements. In the aftermath of corporate accounting scandals involving large scale destruction of documents at WorldCom and Enron, Congress passed the Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745, 758 (2002) (codified in scattered

a duty to preserve, such as a company document retention policy;[26] or (3) a common law obligation to preserve evidence when litigation is filed, threatened, or becomes reasonably foreseeable.[27] Statutory and regulatory obligations to preserve evidence, by their very nature, provide reasonably clear guidelines for meeting that obligation.[28] The extent of a document retention policy is based upon a company's

---

sections of 11, 15, 18, 28 and 29 U.S.C. (Supp. IV 2004)), a corporate responsibility bill that imposes specific document and information retention requirements. *See, e.g.*, 18 U.S.C. §§ 1519, 1520 (Supp. IV 2004) (imposing criminal penalties for the destruction of information subject to preservation under the Sarbanes-Oxley Act); *see also* Private Securities Litigation Reform Act (PSLRA), 15 U.S.C. § 78u-4(b)(3) (2000) (requiring parties to preserve evidence during any stay of litigation). In light of requirements under the PSLRA, a court denied a request for a preservation order. *See* In re Tyco Int'l, Ltd. Sec. Litig., No. 00-MD-1335-B, 2000 U.S. Dist. LEXIS 11659, at *15 (D.N.H. July 27, 2000). See also 17 C.F.R § 240.17a-4(b)(4) (2006), a Securities and Exchange Commission regulation requiring registered broker-dealers to retain copies of all business-related communications, including all forms of digital communications. Similar rules regulate the accounting industry, 26 C.F.R. §§ 1.6060-1, 1.6107-1 (2006), and the banking industry, 12 C.F.R. §§ 202.12, 204.3, 208.20, 220.3, 344.4, 353.3 (2006). *See generally* Mary Kay Brown & Paul D. Weiner, *Digital Dangers: A Primer on Electronic Evidence in the Wake of Enron*, 74 PA. BAR ASSOC. Q. 1, 5 (2003) (stating that evidence destroyed under an organization's retention policy does not release a party from its preservation duty); Lino Lipinsky et al., *Duty to Preserve Electronic Evidence After Enron and Andersen*, 32 COLO. LAW. 55, 56 (2003) (explaining the criminal implications Arthur Andersen faced after the accounting firm destroyed "voluminous amounts of paper and electronic documents that could have been relevant" to the SEC's Enron investigation).

26. Several commentators have addressed the importance of corporate records retention programs. *See* Einar Rowan, *Document Management in the Digital Age*, LEGAL TIMES (2004), http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=1084824756760; Kevin F. Brady & Matthew I. Cohen, *Protecting Against Claims of Spoliation: A Well-Crafted Record-Retention Policy Can Reduce the Risk of Losing Against Such Charges and Sanctions Motions*, NAT'L L.J., July 5, 2004, at S1; John M. Fedders & Lauryn H. Guttenplan, *Document Retention and Destruction: Practical, Legal and Ethical Considerations*, 56 NOTRE DAME LAW. 5 (1980); Christopher V. Cotton, Note, *Document Retention Programs for Electronic Records: Applying A Reasonableness Standard to the Electronic Era*, 24 J. CORP. L. 417 (1999).

27. *Fujitsu Ltd.*, 247 F.3d at 436 (citing *Kronisch*, 150 F.3d at 126).

28. For example, securities regulations include detailed descriptions of required record keeping:

> (a) Every member, broker and dealer subject to § 240.17a-3 shall preserve for a period of not less than six years, the first two years in an easily accessible place, all records required to be made pursuant to paragraphs § 240.17a-3(a)(1), (a)(2), (a)(3), (a)(5), (a)(21), (a)(22), and analogous records created pursuant to paragraph § 240.17a-3(f).
>
> (b) Every member, broker and dealer subject to § 240.17a-3 shall preserve for a period of not less than three years, the first two years in an easily accessible place:
>
> (1) All records required to be made pursuant to § 240.17a-3(a)(4), (a)(6), (a)(7), (a)(8), (a)(9), (a)(10), (a)(16), (a)(18), (a)(19), (a)(20), and analogous records created pursuant to § 240.17a-3(f).
>
> (2) All check books, bank statements, cancelled checks and cash reconciliations.
>
> (3) All bills receivable or payable (or copies thereof), paid or unpaid, relating to the business of such member, broker or dealer, as such.
>
> (4) Originals of all communications received and copies of all communications sent (and any approvals thereof) by the member, broker or dealer (including inter-office memoranda and communications) relating to its business as such, including all communications which are subject to rules of a self-

business need and applicable government requirements.[29] Yet of the three justifications, the third justification based on the existence of pending or actual litigation is the most troublesome in determining when the duty to preserve is triggered and the scope of the duty. While the case law has developed general guidelines as to when the duty exists and the scope of the duty, these guidelines are more difficult to follow when electronic information is involved.

A series of rulings by Judge Scheindlin in the *Zubulake* litigation have shaped the contours of electronic discovery and provide an example of how electronic discovery issues emerge within litigation.[30] The plaintiff, Laura Zubulake, an equities trader with UBS, filed a gender discrimination claim against the company for failure to promote and retaliation under federal, state and city laws.[31] Zubulake first filed a gender discrimination claim with the Equal Employment Opportunity Commission on August 16, 2001.[32] Six months later, Zubulake filed her complaint in the federal district court for the Southern District of New York.[33]

During the course of discovery, the plaintiff learned that although the requested relevant e-mails had been deleted, the e-mails might still exist on backup tapes.[34] UBS identified ninety-four potentially responsive backup tapes but argued that the tapes were not accessible and that to search the tapes for responsive e-mails would

---

regulatory organization of which the member, broker or dealer is a member regarding communications with the public. As used in this paragraph (b)(4), the term communications includes sales scripts.

17 C.F.R. § 240.17a-4 (2006).

29. However, a recent survey suggests that, while improving, traditional document retention policies struggle with the challenges posed by digital information. *See* ROBERT F. WILLIAMS & LORI J. ASHLEY, 2005 ELECTRONIC RECORDS MANAGEMENT SURVEY: A RENEWED CALL TO ACTION 18 (2005), *available at* http://www.merresource.com/pdf/survey2005.pdf [hereinafter COHASSET SURVEY]. The survey was co-sponsored by the Association of Information and Image Management and the Association of Records Managers and Administrators. *See id.* at 63. Nearly 2,100 organizations responded to the survey. *Id.* at 26. The authors describe the "sea change" underway in records management as "the transformation of records management—from the paradigm of media-centric records, where management was based on observable physical location controlled by humans, to the age of digital information and content-centric records management, where the management process is based on invisible logical location controlled by computers." *Id.* at 7.

30. *Zubulake I*, 217 F.R.D. 309 (S.D.N.Y. 2003). The court in *Zubulake I* also acknowledged the role of the *Sedona Principles* in furnishing practical guidance on electronic discovery, although not agreeing with all of the recommendations. *Id.* at 320 n.61. The Sedona Conference, a non-profit organization devoted to the study of law and policy, assembled a small group of lawyers and consultants specializing in issues related to the discovery of electronic evidence, which held its first meeting in October 2002. THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PROD. 1 (Jonathan M. Redgrave et al. eds., 2003), *available at* http://www.thesedonaconference.org/ [hereinafter SEDONA PRINCIPLES]. In March 2003, the group produced the *Sedona Principles*, containing a thorough analysis of electronic discovery issues and offering fourteen preliminary principles to guide practitioners and courts in addressing those issues. *Id.* at 9–10.

31. *Zubulake I*, 217 F.R.D. at 311.

32. *Id.* at 312.

33. *Id.*

34. *Id.* at 313.

be costly and time-consuming.[35] In *Zubulake I*, the court addressed the issue of cost-shifting in electronic discovery and promulgated a new seven factor test for determining when discovery costs should be shifted to the requesting party.[36] Because the evidentiary record was sparse, the court ordered UBS to bear the costs of restoring a sample of the backup tapes.[37] In *Zubulake v. UBS Warburg LLC (Zubulake III)*, based on the results of the sample restoration, and after applying the cost-shifting analysis, the court ordered the parties to share the cost of restoring designated UBS backup tapes.[38] In the restoration effort, the parties discovered that certain backup tapes were missing and some isolated e-mails had been deleted from the system.[39]

As a result of this destruction of potentially relevant evidence, the litigants came before Judge Scheindlin again when the plaintiff sought sanctions against UBS for its failure to preserve the missing backup tapes and deleted e-mails.[40] In *Zubulake IV*, the court defined the contours of the duty to preserve evidence and the consequences for failing to meet those obligations.[41] Although the court found that UBS was under a duty to preserve the backup tapes, and that the company

---

35. *Id.* at 317. The plaintiff in *Zubulake* realized the defendant's discovery production was incomplete when the production failed to include e-mails that the plaintiff already had. *Id.* In a more recent case, however, this argument was unsuccessful. *See* Washington v. Thurgood Marshall Academy, 232 F.R.D. 6, 11 (D.D.C. 2005) (refusing to compel production of e-mails when the plaintiff had produced over fifteen relevant e-mails and the defendant had only produced five).

36. The court modified the cost-shifting analysis from *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 429 (S.D.N.Y. 2002), *aff'd*, 53 Fed. R. Serv. 3d (West) 296 (2002), because Judge Scheindlin found that the *Rowe* factors, as applied, lacked neutrality. *Zubulake I*, 217 F.R.D. at 320–21. Therefore, *Zubulake I* offered a new cost-shifting analysis which included a seven factor test to determine whether cost-shifting was appropriate:

1. The extent to which the request is specifically tailored to discover relevant information;
2. The availability of such information from other sources;
3. The total cost of production, compared to the amount in controversy;
4. The total cost of production, compared to the resources available to each party;
5. The relative ability of each party to control costs and its incentive to do so;
6. The importance of the issues at stake in the litigation; and
7. The relative benefits to the parties of obtaining the information.

Id. at 322. Commentators have further analyzed the *Zubulake I* cost-shifting analysis. *See generally* James M. Evangelista, *Polishing the "Gold Standard" on the E-Discovery Cost-Shifting Analysis:* Zubulake v. UBS Warburg, LLC, 9 J. TECH. L. & POL'Y 1 (2004) (discussing weakness in the *Rowe* test and the increasing significance of the *Zubulake* decisions in the area of electronic discovery). Although the cost-shifting analysis is not the focus of this Article, the possibility that courts might shift the discovery expense to the requesting party is a significant concern. *See* Wiginton v. CB Richard Ellis, Inc. (*Wiginton II*), 229 F.R.D. 568, 577 (N.D. Ill. 2004) (applying the *Zubulake* factors, the court ordered the employer to bear 25% and the employee 75% of the costs required to restore backup tapes, search data, and transfer information to a data viewer).

37. *Zubulake I*, 217 F.R.D. at 324.

38. 216 F.R.D. 280, 291 (S.D.N.Y. 2003).

39. *Id.* at 287, 290 (clarifying that cost-shifting analysis was strictly limited to the costs associated with making UBS's "inaccessible" archived data "accessible").

40. Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 215 (S.D.N.Y. 2003).

41. *Id.* at 217–19.

destroyed the tapes with the "requisite culpability," it found that the plaintiff could not "demonstrate that the lost evidence would have supported her claims."[42] Therefore, the court refused to give an adverse inference instruction to the jury but ordered UBS to bear the cost of deposing "witnesses for the limited purpose of inquiring into issues raised by the destruction of evidence and any newly discovered e-mails."[43] The saga continued in *Zubulake v. UBS Warburg LLC* (*Zubulake V*),[44] when the parties appeared for a second time before Judge Scheindlin for sanctions based on the information learned from the previously ordered depositions.[45] In *Zubulake V*, the court addressed "counsel's obligation to ensure that relevant information is preserved by giving clear instructions to the client to preserve such information and . . . a client's obligation to heed those instructions."[46] Finally, a jury awarded Laura Zubulake $20.1 million in punitive damages and $9.1 million in compensatory damages.[47] The defendant will likely appeal the award. The *Zubulake* litigation and the decisions that resulted carve out the many issues and challenges surrounding electronic discovery, particularly the duty to preserve electronic evidence.

A. The Duty to Preserve Evidence Generally

The duty to preserve evidence in the face of anticipated litigation is well established in federal law. All federal circuits recognize this duty[48] and as Judge Scheindlin notes in *Zubulake IV*, "Identifying the boundaries of the duty to preserve involves two related inquiries: *when* does the duty to preserve attach, and *what* evidence must be preserved?"[49] Both inquiries ultimately hinge on when a party receives notice of anticipated litigation; the specificity of that notice will dictate what needs to be preserved.

1. When Is the Duty to Preserve Triggered?

The duty to preserve evidence is triggered when an organization reasonably anticipates litigation.[50] Within the context of possible civil litigation, the duty to

42. *Id.* at 222.
43. *Id.*
44. 229 F.R.D. 422 (2004).
45. *Id.* at 424, 426.
46. *Id.* at 424.
47. *Verdicts and Settlements*, NAT'L L.J., Apr. 11, 2005, at 16.
48. *See supra* note 24.
49. Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 216 (S.D.N.Y. 2003).
50. *Id.* at 217. *See also* Wiginton v. CB Richard Ellis, Inc. (*Wiginton I*), No. 02 C 6832, 2003 WL 22439865, at *4 (N.D. Ill. Oct. 27, 2003) ("A party has a duty to preserve evidence over which it had control and 'reasonably knew or could reasonably foresee was material to a potential legal action.'") (quoting China Ocean Shipping (Group) Co. v. Simone Metals, Inc., 1999 WL 966443, at *3 (N.D. Ill. Sept. 30, 1999)); Thompson v. U.S. Dept. of Hous. & Urban Dev., 219 F.R.D. 93, 100 (D. Md. 2003) (citing *Zubulake IV* for the proposition that the duty to preserve evidence is triggered when the party reasonably anticipates litigation).

preserve evidence can arise as early as the time of the event that ultimately leads to litigation. More commonly, however, the duty to preserve arises when a party has been served the complaint.[51] Once pleadings have been filed and parties have responded, the litigants should have notice of the disputed issues and be aware of what information might be material to the litigation. At the very latest, the duty is triggered when parties receive specific discovery requests. Outside the boundaries of these specific stages of litigation, however, the duty may be triggered even before a complaint is filed.

Some events carry the clear implication of potential disputed issues and possible litigation, such as a major accident on a common carrier. In contrast, day-to-day business activities contain innumerable possibilities for future litigation, including employment, product liability, business, and regulatory litigation. Under these circumstances, courts look for significant signs of imminent litigation prior to the filing of a complaint and only impose a duty to preserve evidence when the signs are clear.[52] Courts consider the point at which a party knew or should have known that litigation was imminent and impose a duty to preserve based on that notice.[53]

Courts are not in agreement as to when a party should be charged with sufficient notice of a claim to trigger the preservation obligation. Although some courts have accepted common signs of looming litigation to include communication with the adverse parties[54] or when related litigation is filed,[55] other courts have found that the duty should not adhere until a specific discovery request has been

---

51. *See* Computer Assoc. Int'l Inc. v. Am. Fundware, Inc., 133 F.R.D. 166, 169–70 (D. Colo. 1990) (issuing a default judgment against a party that willfully destroyed electronic evidence after litigation began).

52. For example, when an employee files a charge of employment discrimination with the EEOC, an employer would have notice of anticipated litigation and the duty to preserve material documents would attach. *Zubulake IV*, 220 F.R.D. at 216; *see also* E*TRADE Sec. LLC v. Deutsche Bank AG, 230 F.R.D. 582, 589 (D. Minn. 2005) (finding that duty to preserve electronic documents concerning a fraudulent securities loan scheme was triggered when the party received notice that a bankruptcy court was investigating the scheme). One court stated that the "definition of when a party anticipates litigation is elusive" and suggested that a "helpful analytical tool is the more widely developed standard for anticipation of litigation under the work product doctrine." Samsung Elecs. Co. v. Rambus, Inc., No. Civ.A. 3:05CV406, 2006 WL 2038417, at *15 (E.D. Va. July 18, 2006).

53. Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998) ("This obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation—most commonly when suit has already been filed, . . . but also on occasion in other circumstances, as for example when a party should have known that the evidence may be relevant to future litigation."), *aff'd sub nom.* Kronisch v. Gottlieb, 213 F.3d 626 (2d Cir. 2000).

54. *See* Wm. T. Thompson Co. v. Gen. Nutrition Corp., 593 F. Supp. 1443, 1446 (C.D. Cal. 1984) (finding that pre-litigation correspondence between the parties' counsel put defendant on notice that records it destroyed were relevant to the litigation); *see also* Capellupo v. FMC Corp., 126 F.R.D. 545, 548 (D. Minn. 1989) (finding that evidence of pre-litigation meetings and internal memoranda generated by the defendant demonstrated that the defendant was on notice of the duty to preserve evidence before the actual filing of the claim).

55. For example, in *United States* ex rel. *Koch v. Koch Industries, Inc.*, 197 F.R.D. 463, 482 (N.D. Okla. 1998), a court recognized the defendant's pre-litigation duty to preserve evidence based on other parties' participation in litigation involving the same circumstances.

made.[56] More recent decisions indicate, however, that courts are increasingly unsympathetic toward claims that a party did not have sufficient notice of the need to preserve certain information until another party specifically requested that information.[57] When a party knows it will need specific information to prove its case and that information is under the adverse party's control, more formal steps may be needed to ensure notice of the need for pre-litigation preservation of evidence, such as the filing of motions for preliminary injunctions, preservation orders, or ex parte orders.[58]

The timing of the notice also impacts the specificity of the duty and the court's expectation of what the party should have preserved. During early pre-litigation stages, courts impose a general duty to preserve evidence but limit this preservation obligation by noting that a party does not have a duty to preserve every scrap of evidence. Judge Scheindlin addressed the duty in *Zubulake IV*: "Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic document, and every backup tape? The answer is clearly, 'no.' Such a rule would cripple large corporations . . . that are almost always involved in litigation."[59] As the litigation advances, however, and the issues are narrowed, either by the pleadings or by specific discovery requests, the duty to preserve evidence becomes more specific and parties face an increased risk of sanctions if they do not observe the preservation duty. Thus, a common issue in determining whether there is a duty to preserve evidence hinges upon the parties' actions and the point in time the duty to preserve arises.

2. *The Scope of the Duty to Preserve*

The scope of the duty to preserve within the context of civil litigation is framed by the relevance provisions within the Federal Rules of Evidence and the discovery provisions within the Federal Rules of Civil Procedure. Under the Federal Rules of Evidence, "relevant evidence" is "evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence."[60] For purposes of discovery, the Federal Rules of Civil Procedure describe relevant material more broadly as "any matter, not privileged, that is relevant to the claim or defense of any party, ... [The] [r]elevant information need not be admissible at the trial if the

---

56. *See, e.g.*, Hansen v. Dean Witter Reynolds Inc., 887 F. Supp. 669, 676 (S.D.N.Y. 1995) (holding that, although it was a "close question," neither the filing of the employment discrimination complaint, nor the correspondence received from the EEOC and the New York State Division of Human Rights, put the defendant on notice that it had a duty to preserve trading tickets involving the plaintiff); Szymanska v. Abbott Labs., No. 93 C 3033, 1994 WL 118154, at *10 n.7 (N.D. Ill. Mar. 29, 1994) (holding that an employment discrimination complaint did not put employer on notice that it had a duty to preserve records relating to other employees).

57. *See Zubulake IV*, 220 F.R.D. at 216.

58. *See* COHEN & LENDER, *supra* note 4, § 2.03, at 2–6; *see also infra* Part IV (discussing in detail such proactive steps to ensure compliance with the duty to preserve).

59. *Zubulake IV*, 220 F.R.D. at 217.

60. FED. R. EVID. 401.

discovery appears reasonably calculated to lead to the discovery of admissible evidence."[61] Relevancy for purposes of the duty to preserve is defined as what a party "knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request."[62] Moreover, the Federal Rules of Civil Procedure indicate that the duty to preserve, and ultimately to produce relevant evidence, arises with the filing of the complaint and extends to electronic as well as paper forms of evidence.[63] "The law is clear that data in computerized form is discoverable even if paper 'hard copies' of the information have been produced . . . . [T]oday it is black letter law that computerized data is discoverable if relevant."[64] Under the initial disclosure rules, a party must produce evidence "based on the information then reasonably available to it and is not excused from making its disclosures because it has not fully completed its investigation of the case or because it challenges the sufficiency of another party's disclosures or because another party has not made its disclosures."[65]

Rule 34 of the Federal Rules of Civil Procedure defines "documents"[66] subject to discovery as including "data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form."[67] The rules that apply to traditional paper discovery also

---

61. FED. R. CIV. P. 26(b)(1).

62. Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 72 (S.D.N.Y. 1991) (quoting Wm. T. Thompson Co. v. Gen. Nutrition Corp., 593 F. Supp. 1443, 1455 (C.D. Cal. 1984)).

63. *See* FED. R. CIV. P. 34 advisory committee's notes (1970) (extending the rules of discovery to digital forms of information).

64. Anti-Monopoly, Inc. v. Hasbro, Inc., 1995-2 Trade Cases 75,898, 75,898 (S.D.N.Y. 1995); *see also* Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 652 (D. Minn. 2002) (finding the defendant had a duty to preserve digital records lost through the normal use of the defendant's computer system).

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

66. Commentators have criticized the continued use of the term documents in the Federal Rules of Civil Procedure:

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

Lisa M. Arent et al., *EDiscovery: Preserving, Requesting & Producing Electronic Information*, 19 SANTA CLARA COMPUTER & HIGH TECH. L.J. 131, 133 n.5 (2002).

67. FED. R. CIV. P. 34(a). *See* Noyes, *supra* note 3, at 643 n.272 (quoting FED. R. CIV. P. 34 advisory committee's notes (1970) (affirming that digital documents were in the purview of Rule 34 and that courts could handle the details involved in accessing and producing such documents)). The Advisory Committee's notes recognize courts' authority:

> [C]ourts have ample power under Rule 26(c) to protect respondent against undue burden or expense, either by restricting discovery or requiring that the discovering party pay costs. Similarly if the discovering party needs to check the electronic source itself, the court may protect respondent with respect to the preservation of his records, confidentiality of nondiscoverable matters, and costs.

apply to electronic discovery.[68] "Courts now routinely require litigants to demonstrate good faith efforts to identify discoverable electronic data, and to inform opposing counsel when data is available for production in electronic form."[69] With respect to discovery obligations, litigants and their attorneys can hardly claim they are unaware that digital information might be subject to discovery.

Under the proposed amendments to Rule 34, discovery clearly extends to electronic information.[70] The title of Rule 34 will change to "Production of Documents, *Electronically Stored Information*, and Things and Entry Upon Land for Inspection and Other Purposes."[71] Rather than continue to stretch the definition of "document" within Rule 34, the proposed amendment makes the inclusion of electronic information explicit and allows parties to "specify the form or forms in which electronically stored information is to be produced."[72]

B. Preservation of Electronic Information

Electronic information, by its very nature, poses interesting challenges for litigants and courts as they attempt to define the boundaries of the duty to preserve. "An electronic file contains easily accessible and highly reliable corporate knowledge, leaves a metadata chronology of key dates, comments between collaborators and, in effect, a knowledge map of who knew what, and when it

---

FED. R. CIV. P. 34 advisory committee's notes (1970). *See generally* Hon. Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 up to the Task?*, 41 B.C. L. REV. 327, 346 (2000) (emphasizing that discovery of electronic information "proceeds under the same framework as discovery of any other information under Rule 34").

68. Linnen v. A.H. Robins Co., 10 Mass. L. Rep. 189, 192 (Mass. Super. Ct. 1999) ("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 any office file cabinet."); *see also* Kleiner v. Burns, 48 Fed. R. Serv. 3d (West) 644, 649 (D. Kan. 2000) (noting that discoverable data may include "voice mail messages and files, back-up voice mail files, e-mail messages and files, backup e-mail files, deleted e-mails, data files, program files, backup and archival tapes, temporary files, system history files, web site information stored in textual, graphical or audio format, web site log files, cache files, cookies, and other electronically-recorded information."); Simon Prop. Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 639 (S.D. Ind. 2000) (finding that the plaintiff was entitled to the discovery of the defendant's relevant deleted computer files).

69. Virginia Llewellyn, *Electronic Discovery Best Practices*, 10 RICH. J.L. & TECH. 51, ¶ 3 (2004) (citing *In re* Livent, Inc. Noteholders Sec. Litig., 210 F.R.D. 512 (S.D.N.Y. 2003); *In re* Bristol-Myers Squibb Sec. Litig., 205 F.R.D. 437 (D.N.J. 2002)).

70. JUDICIAL CONFERENCE REPORT, *supra* note 19, app. C, at 70 (containing text of proposed rules).

71. *Id.* (emphasis added).

72. *Id.* app. C, at 70–71. The proposed rule also states that "if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable; and . . . a party need not produce the same electronically stored information in more than one form." *Id.* app. C, at 73.

became known."[73] It is therefore not surprising that electronically stored information is of such interest to litigants. Litigants are well aware that electronic information may contain a wealth of data. In an effort to reinforce the importance of digital information, the American Bar Association (ABA) amended the discovery standards by extending the duty to preserve potentially relevant documents to electronic sources of information.[74]

---

73. COHEN & LENDER, *supra* note 4, app. 1B, at 1-49 to -50. The authors note the following key distinctions about digital information:

- Electronic information that has been "deleted" by common programs is often not erased and may be recoverable;
- Common computer programs often generate numerous copies of electronic documents without the knowledge of the user;
- "Back-ups" of many types of electronic information periodically made to guard against systems failures are often retained and archived;
- Electronic versions of E-mails and word processing documents may reveal information (such as draft versions, "bcc" recipients, etc.) that exist only in electronic form and not on hard copies;
- Even when voluminous, electronic information may be easier to search and analyze than paper documents;
- People are often casual and careless when communicating via E-mails as opposed to hard copy memoranda and correspondence.

Id. app. 1A, at 1-9.

74. AM. BAR ASS'N, CIVIL DISCOVERY STANDARDS, 29, at 57 (rev. 2004), *available at* http://www.abanet.org/litigation/discoverystandards/2004civildiscoverystandards.pdf. The Standard 29 states,

> In identifying electronic data that parties may be called upon, in appropriate circumstances, to preserve or produce, counsel, parties and courts should consider:
>
> i. The following types of data:
>
> A. Email (including attachments);
> B. Word processing documents;
> C. Spreadsheets;
> D. Presentation documents;
> E. Graphics;
> F. Animations;
> G. Images;
> H. Audio, video and audiovisual recordings;
> I. Voicemail.
>
> ii. The following platforms in the possession of the party or a third person under the control of the party (such as an employee or outside vendor under contract):
>
> A. Databases;
> B. Networks;
> C. Computer systems, including legacy systems (hardware and software);
> D. Servers;
> E. Archives;
> F. Back up or disaster recovery systems;
> G. Tapes, discs, drives, cartridges and other storage media;
> H. Laptops;
> I. Personal computers;
> J. Internet data;
> K. Personal digital assistants;

In addition to the added value of digital information over the comparable paper document, digital information continues to be accessible long after attempts to delete the information.[75] Despite consistent court rulings that deleted electronic evidence is fully discoverable,[76] some litigants try to avoid their discovery obligations through digital destruction. For example, in *Anderson v. Crossroads Capital Partners*,[77] the plaintiff in a sexual harassment and whistleblower suit used a file-wiping program, "CyberScrub," to destroy potential evidence.[78] The court found that the plaintiff's "exceedingly tedious and disingenuous claim of naivete . . . defies the bounds of reason."[79] In turn, litigants sometimes question a court's understanding of the demands of electronically stored information when these courts require litigants to go to great lengths and expense to retrieve information of questionable value.[80] While there is a growing sophistication concerning the characteristics of electronic information and its storage methods, many courts and litigants lack an adequate understanding of the capabilities and limits of electronic information.

This lack of understanding may lead courts and litigants to impose unreasonable demands on the preservation and accessibility of electronic information. As technology continues to improve and evolve, parties have a myriad of choices as to how information is created, stored, and preserved. These choices have significant consequences for determining the scope of the duty to preserve. Therefore, to understand the preservation obligations, courts, litigants, and

---

L. Handheld wireless devices;
M. Mobile telephones;
N. Paging devices; and
O. Audio systems, including voicemail.

Id. 29(a), at 57–58. The standard also notes that data subject to discovery might also include "potentially producible electronic data . . . that have been deleted but can be restored." *Id.* 29(a)(iii).

75. Deleted electronic information is not physically erased. Instead, space occupied by the deleted file on a computer hard drive is "marked as available for reuse." COHEN & LENDER, *supra* note 4, app. 1A, at 1-34. Until the space is completely written over, the electronic information is still retrievable. *Id.*

76. *See* Simon Prop. Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 640 (S.D. Ind. 2000); Ill. Tool Works, Inc. v. Metro Mark Products, Ltd., 43 F. Supp. 2d 951, 958–59 (N.D. Ill. 1999).

77. No. Civ.01-2000 ADM/SRN, 2004 WL 256512 (D. Minn. Feb. 10, 2004).

78. *Id.* at *2.

79. *Id.* at *8 (citing Pope v. Fed. Express Corp., 974 F.2d 982, 984 (8th Cir. 1992), *aff'd*, 49 F.3d 1327 (8th Cir. 1995)); *see also* Minn. Mining & Mfg. Co. v. Pribyl, 259 F.3d 587, 606 n.5 (7th Cir. 2001) (finding defendant committed spoliation of evidence by downloading six gigabytes of music onto a laptop in an attempt to eradicate deleted files).

80. *See, e.g.*, Medtronic Sofamor Danek, Inc. v. Michelson, No. 01-2373-M1V, 2003 U.S. Dist. LEXIS 8587, at *8–9, *24–28 (W.D. Tenn. May 13, 2003) (describing the plaintiff's concern that e-discovery costs would reach millions of dollars). *See generally* Sonia Salinas, Note, *Electronic Discovery and Cost Shifting: Who Foots the Bill?*, 38 LOY. L.A. L. REV. 1639, 1640 (2005) ("Due to the protests of burdened parties and legal scholars, the established 'producer pays' rule has come into question.").

attorneys must understand how electronic information is created, modified, and stored.[81]

1. The Lifeline of Digital Information

Within an organization, the lifeline of electronic information begins as active data in the creation of a work-in-progress, changes to replicant data on the user's computer, is stored in backup or archival systems, and finally as residual data.[82] Whether a computer user creates a word processing document, spreadsheet, database, or e-mail message; enters information in an electronic calendar or contacts list; or uses a communication system such as voice mail or instant messaging, the end result is active data. The data is termed "active" because it can easily be retrieved and modified.[83] As this digital information is created, many information systems create replicant data on the user's hard drive to provide a backup copy in case of a computer malfunction.[84] However, organizations differ as to whether replicant data is created, where it is stored, and how long it is stored. Beyond the individual computers where information is created and stored, many organizations operate within an information network where active data is routinely backed up on magnetic tape or other removable media.[85] When a user deletes digital information, it may still exist as residual data on the individual computer, or it may have been captured on the organization's backup system.[86]

Confusion exists, however, between backup and archival tapes. Although both backup tapes and archive tapes are intended to provide access to information in the event of system wide failure, backup tapes typically, are subject to a routine schedule of daily, weekly, and monthly backups.[87] Organizations may choose to back up electronic information differently depending on the source. For example, e-mail may be managed on a different backup system than word processing documents, spreadsheets, and databases.[88] Backup tapes are only kept for a certain amount of time, and then recycled on varying schedules.[89] Archival tapes may also

---

81. For an in-depth explanation of electronic information and how it is stored, see COHEN & LENDER, *supra* note 4, app. 1A, at 1-34 to -40. Additionally, Microsoft's public comments to the Advisory Committee on the proposed amendments to the discovery rules include not only helpful explanations of electronic information, but also a graphical display of the inner workings of a typical corporate internal network. Letter from Microsoft Corporation to Peter G. McCabe, Secretary, Committee on Rules of Practice & Procedure (Dec. 16, 2004), *available at* http://www.uscourts.gov/rules/e-discovery/04-CV-001.pdf.

82. Martin H. Redish, *Electronic Discovery and the Litigation Matrix*, 51 DUKE L.J. 561, 584 (2001) (describing the five types of data as active, replicant, archival or backup, residual, and hidden or embedded).

83. *Id.*

84. *Id.*

85. *See id.* at 585.

86. COHEN & LENDER, *supra* note 4, app. 1A, at 1-42.

87. *See id.*

88. *See* SEDONA GUIDELINES, *supra* note 1, app. E, at 84 (recognizing the importance and the difficulty in managing e-mails).

89. COHEN & LENDER, *supra* note 4, app. 1A, at 1-34.

include backup tapes, but in some organizations, archives may be limited to critical organizational information. Archives may be stored differently than backup tapes.[90] Thus, while all information may be backed up, only some information will be archived. The choice of where and how data is stored directly affects the accessibility of data and the ease of preservation and retrieval.

This distinction between archives and backup tapes was an issue in *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.*[91] Morgan Stanley argued that the opposing party wanted the court "'to order a massive safari into the remote corners of MS & Co.'s email backup systems' and represented that '[t]he restoration efforts demanded . . . would *cost at least hundreds of thousands of dollars* and require several months to complete.[']"[92] Despite Morgan Stanley's representations of the difficulties it would encounter in searching e-mail backup tapes, much of its e-mail system was in the process of being transferred, or had already been transferred, to an easily searchable archive.[93] The court sanctioned the company for its wrongful conduct by imposing a partial default judgment, which ultimately resulted in a $1.45 billion fraud verdict.[94]

In *Quinby v. WestLB AG*,[95] arguably similar conduct resulted in no sanctions. The court addressed the difficulties encountered when the plaintiff in a gender discrimination suit attempted to learn the location and accessibility of potentially relevant e-mails.[96] The defendant first responded that retrieval of the e-mails would be "'extremely costly, time-consuming and unduly burdensome'" and that an expert had been hired to assist with collecting the information.[97] The plaintiff later learned that a large quantity of the e-mails had existed on a more accessible backup system but had been converted to a less accessible system, leading the plaintiff to argue that affidavits describing the expense and burden of accessing the e-mails were misleading.[98] The court dismissed the plaintiff's arguments, noting that the duty to preserve electronic data does not include "a duty to keep the data in an accessible

---

90. For a more complete explanation of the technical differences between backup tapes and archives, see SEDONA GUIDELINES, *supra* note 1, app. E, at 83–90. Recent litigation has demonstrated the possibility for confusion when an organization has multiple backup systems. *See* Quinby v. WestLB AG, No. 04Civ.7406(WHP)(HBP), 2005 WL 3453908, at *8, *10 (S.D.N.Y. Dec. 15, 2005) (declining to grant sanctions when a party converted data in an accessible backup system to an inaccessible backup system); Keir v. UnumProvident Corp., No. 02 Civ. 8781(DLC), 2003 WL 21997747, at *5, *9 (S.D.N.Y. Aug. 22, 2003) (describing how defendant had inadvertently destroyed requested e-mails on backup tapes).

91. No. CA 03-5045 AI, 2005 WL 674885, at *5 (Fla. Cir. Ct. Mar. 23, 2005).

92. *Id.* at *2.

93. *Id.* at *5 n.11.

94. *Id.* at *9; Paul D. Boynton, *E-Discovery Mistakes Haunt Morgan*, INTERNET L. July 2005, at 1.

95. 2005 WL 3453908, at *2–3.

96. No. 04Civ.7406(WHP)(HBP), 2005 WL 3453908, at *1 (S.D.N.Y. Dec. 15, 2005).

97. *Id.* at *2. The defendant estimated that the ninety-eight yearly backup tapes would cost $106,000 to restore and the more than 3,700 other backup tapes from 2004 would cost another $2.8 million to restore. *Id.* at *2–3.

98. *Id.* at *3.

format."[99] Thus the court declined to sanction the defendant for converting data from an accessible to an inaccessible format, even though the defendant anticipated litigation.[100] The lifeline of digital information, as it shifts from accessible active data to inaccessible data, presents a continuing challenge to the scope of the duty to preserve.

2. *Hidden Data Within Digital Information*

Included in digital information is "metadata," which provides information concerning file dates, authors, source locations, and e-mail and printer routing information.[101] While metadata may appear in the digital version of a document, it does not appear on the printed page.[102] Therefore, according to some experts, the viewability of the information should be a determining factor in whether metadata is presumptively treated as part of a document.[103] This view, however, was rejected in *Armstrong v. Executive Office of the President*,[104] when the court held that the preservation obligation under the Federal Records Act was not properly discharged when paper printouts did not reflect the metadata information contained in the electronic document.[105] The court stated that:

> [The] paper rendering will not, however, necessarily include all the information held in the computer memory as part of the electronic document. Directories, distribution lists, acknowledgements of receipts and similar materials do not appear on the computer screen—and thus are not reproduced when users print out the information that appears on the screen. Without this "non-screen" information, a later reader may not be able to glean

---

99. *Id.* at *8 n.10.

100. *Id.* at *8 n.10. *But see* Treppel v. Biovail Corp., 233 F.R.D. 363, 372 n.4 (S.D.N.Y. Feb. 6, 2006) (citing Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 110 (2d Cir. 2002), (disagreeing with the court in *Quinby* and noting that "conduct that hinders access to relevant information is sanctionable, even if it does not result in the loss or destruction of evidence").

101. For a thorough explanation of metadata, see SEDONA GUIDELINES, *supra* note 1, app. E, at 80–82. *See also* Microsoft Office Online, Find and Remove Metadata (Hidden Information) in Your Legal Documents, http://office.microsoft.com/en-us/assistance/HA010776461033.aspx (last visited Oct. 3, 2006) (describing metadata, listing examples, and providing articles on removing metadata).

102. For example, some metadata information, such as a file's creation date or its size, may not appear on the actual document when viewed on the screen. Clicking on the "properties" of the document or viewing a list of electronic documents within a file folder will display the metadata. The court in *Momah v. Albert Einstein Medical Center*, an employment discrimination case where the plaintiff sought to prove that records had been back-dated, recognized the value of information contained in a list of the files. 164 F.R.D. 412, 418 (E.D. Pa. 1996). While calling the discoverability of metadata a "close question," the court allowed the plaintiff "to access the computer list screen." *Id.*

103. *See generally* SEDONA PRINCIPLES, *supra* note 30, at 30 cmt. 9.a ("The best approach to understanding what is a document is to examine what information is readily available to the computer user in the ordinary course of business.").

104. 1 F.3d 1274 (D.C. Cir. 1993).

105. *Id.* at 1282–87.

> from the hard copy such basic facts as who sent or received a particular message or when it was received. For example, if a note is sent to individuals on a distribution list already in the computer, the hard copy may well include only a generic reference to the distribution list (*e.g.*, "List A"), not the names of the individuals on the list who received the document. Consequently, if only the hard copy is preserved in such situations, essential transmittal information relevant to a fuller understanding of the context and import of an electronic communication will simply vanish.[106]

The same concerns arise when the metadata is removed from an electronic document before the information is produced in discovery.

Files maintained in their "native format"[107] contain the specific metadata used in the program that created the digital file, and different applications may store and treat metadata differently. Files can be saved using applications that preserve the content of the file that would appear in the printed form, but eliminate the metadata from the native format. For example, during document production, litigants often convert electronic documents to "Portable Document Format" (PDF) or TIFF to replace the production of information in its native format, and thereby avoid revealing metadata.[108]

The discoverability of metadata in Excel spreadsheets was directly addressed in *Williams v. Sprint/United Management Company*.[109] During the course of discovery in a class action employment discrimination case, the plaintiffs learned that Excel spreadsheets were produced as TIFF images with all metadata removed,

---

106. *Id.* at 1280.

107. Discovery productions may be viewed in one of several formats: hard copy, native format, or "Tagged Image File Format" (TIFF). Native format is the original file format. For example, the native format for a file created in Word has a .doc file extension while a database spreadsheet created with Excel has an .xls file extension. Many e-mail files, as well as other personal information files, are saved on a computer in their native format with a .pst extension. *See In re* Priceline.com, Inc. Sec. Litig., 233 F.R.D. 88, 89–91 (D. Conn. 2005) (describing the relative merits of native format and providing a protocol for electronic discovery).

108. Although a producing party often favors a TIFF conversion because it can create a "virtual stone age of non-searchable images," depending on how the document is converted, the electronic document can still retain some searchability and background information. *See* Daniel Pelc, *The Top Ten Faux Pas of TIFFs*, LAW PRACTICE TODAY, Sept. 2005, http://www.abanet.org/lpm/lpt/articles/tch09052.html. Because a TIFF conversion typically strips the metadata from the document, parties may argue that this form of production is inadequate. *See In re* Verisign, Inc. Sec. Litig., No. C 02-02270 JW, 2004 WL 2445243, at *1–2 (N.D. Cal. Mar. 10, 2004) (affirming a magistrate's order finding that the production of documents in a TIFF version alone was not sufficient); *see also* Nova Measuring Instruments LTD v. Nanometrics, Inc., 417 F. Supp. 2d 1121, 1123 (N.D. Cal. 2006) (requiring parties to produce documents "in their native file format, with original metadata"); *cf. In re Priceline.com*, 233 F.R.D. at 91 (noting that "TIFF or PDF format is the most secure format for the production of documents"). The court in *In re Priceline.com* favored the use of TIFF or PDF because "[g]iven the sheer volume of information . . . [it] should be conveyed as numbered images so that no inadvertent alterations are made, or more likely, no accusations of alteration can be made, and so that the information can be easily identified." *Id.*

109. 230 F.R.D. 640, 651 (D. Kan. 2005).

thus plaintiffs could not conduct a statistical analysis of the data without going through the "'laborious process of keying in all that data again.'"[110] The defendant argued that the spreadsheet metadata was irrelevant and contained privileged information.[111] The court, however, accepted that there could be "a modest legal presumption in most cases that the producing party need not take special efforts to preserve or produce metadata,"[112] but held that the metadata should be produced "when the producing party is aware or should be reasonably aware that particular metadata is relevant" to the dispute.[113]

In reaching its decision, the court in *Williams* considered the duty to produce metadata within the context of Rule 34(b) of the Federal Rules of Civil Procedure, which states that "'[a] party who produces documents for inspection shall produce them as they are kept in the usual course of business . . . .'"[114] The court also considered how the proposed amendments to Rule 34 might alter its analysis.[115] The proposed amendments to Rule 34(b) add the following language about the production of electronically stored information:

> Unless the parties otherwise agree, or the court otherwise orders,
>
> . . . .
>
> (ii) if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable . . . .[116]

Finding that the proposed amendments to Rule 34 provided little guidance, the court relied heavily on the Sedona Guidelines to define the "emerging standards" on the production of metadata and explained the discovery process when the court orders a party to produce electronic documents as they are maintained in the ordinary course of business:

> [T]he producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective

110. *Id.* at 641–42. Prior to producing the spreadsheets, the defendants used software to "scrub the spreadsheet files to remove the metadata," which would have included "information such as file names, dates of the file, authors of the file, recipients of the file, print-out dates, changes and modification dates, and other information." *Id.* at 644.

111. *Id.* at 651.

112. *Id.* (quoting SEDONA PRINCIPLES, *supra* note 30, 36 cmt. 12.a.).

113. *Id.*

114. *Id.* at 648 (quoting FED. R. CIV. P. 34(b)).

115. *Id.* at 649.

116. JUDICIAL CONFERENCE REPORT, *supra* note 19, app. C, at 73.

> order. The initial burden with regard to the disclosure of the metadata would therefore be placed on the party to whom the request or order to produce is directed. The burden to object to the disclosure of metadata is appropriately placed on the party ordered to produce its electronic documents as they are ordinarily maintained because that party already has access to the metadata and is in the best position to determine whether producing it is objectionable. Placing the burden on the producing party is further supported . . . [because] metadata is an inherent part of an electronic document, and its removal ordinarily requires an affirmative act by the producing party that alters the electronic document.[117]

Thus, the scope of discovery, under certain conditions, extends to the metadata included in the electronic document.

3. *File Duplication in the Digital Environment*

Finally, numerous versions of a digital file can co-exist within an electronic network. An e-mail may exist within the original e-mail files of the sender and recipient, but can also exist in the e-mail files of persons who were copied on the e-mail or persons to whom the e-mail was forwarded. A document created in an electronic environment may have a variety of draft versions that continue to exist, all with their own metadata. The possibility for duplication, as well as numerous drafts, poses challenges for the courts and litigants as they attempt to determine how far the scope of the duty to preserve extends.[118] Just as the "scrubbing" of

---

117. *Williams*, 230 F.R.D. at 652; *see also In re* NYSE Specialists Sec. Litig., No. 03 Civ. 8264(RWS), 2006 WL 1704447, at *1 (S.D.N.Y. June 14, 2006) (ordering all electronic documents to be produced in their native format); Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L., No. 04 C 3109, 2006 WL 665005, at *3 (N.D. Ill. Mar. 8, 2006) (mem.) (ordering defendant to produce the electronic documents in their original format, noting that "TIFF documents do not contain all of the relevant, nonprivileged information"); *In re* Verisign, Inc. Sec. Litig., No. C 02-02270 JW, 2004 WL 2445243, at *2–3 (N.D. Cal. Mar. 10, 2004) (affirming a magistrate's order that documents be produced in their native instead of TIFF format). *But see* CP Solutions PTE, LTD. v. Gen. Elec. Co., No. 3:04cv2150(JBA)(WIG), 2006 WL 1272615, at *4 (D. Conn. Feb. 6, 2006) (refusing to order that e-mails be produced in their native .pst format).

118. For example, in *McGuire v. Acufex Microsurgical, Inc.*, the court considered whether the defendant was subject to sanctions in an employment discrimination case when an employee in the human resources department deleted a portion of an evaluation memorandum written by one of the plaintiff's supervisors. 175 F.R.D. 149, 150 (D. Mass. 1997). The deleted portion described advice the supervisor had given the plaintiff in response to her claims of sexual harassment. *Id.* The paragraph stated in part that the supervisor told the plaintiff that "an attractive woman cannot be one of the guys," and her attempt to include herself was "misconduct on her part." *Id.* at 151–52. The human resources employee deleted the paragraph because it was "inappropriate" to keep this kind of record in a personnel file. *Id.* at 152. The plaintiff first learned of the missing paragraph when the supervisor brought the original memo to a deposition. *Id.* The supervisor had submitted his draft to the Human Resources department on disk; however, all the defendant employer produced from the Human Resources office was the final, edited document. *Id.* The court held that employers are free to edit drafts

metadata from an electronic document can rob the information of important context, so can limitations on the production of duplicate versions of electronic information. The removal of duplicates in an electronic document production (also known as de-duplication or "de-dupe" the records), although not yet addressed by the courts, may involve many of the same issues that have emerged concerning metadata.[119]

4. Accessibility of Digital Information

In addition to the type of digital information stored, how it is stored also impacts on the accessibility of the information. Information collected in a database is organized to allow data retrieval through written "queries."[120] Depending on the design, or lack of design, of the database, information may not be easily retrievable. Recognizing the need to maintain archived information in an accessible format to comply with securities regulations, companies specializing in information management provide archive and backup systems that are easily accessible.[121] As advancements in technology increase accessibility of digital information, courts are hinging a litigant's duty to preserve information on its accessibility.

As information is created and stored, discovery obligations depend upon the accessibility of the information at each stage. In *Zubulake I*,[122] Judge Scheindlin described the five categories of data, from most to least accessible:

1. *Active, online data*: "On-line storage is generally provided by magnetic disk. It is used in the very active stages of an electronic records [sic] life—when it is being created or received and processed, as well as when the access frequency

---

of memos in the sexual harassment context when the edits concern "obvious errors made by someone other than the accused harasser." McGuire v. Acufex Microsurgical, Inc., 175 F.R.D. 149, 155 (D. Mass. 1997). In denying the request for sanctions, the court explained that "[t]o hold otherwise would be to create a new set of affirmative obligations for employers, unheard of in the law—to preserve all drafts of internal memos." *Id.* at 156.

119. *See generally* Jack Seward, *Protecting Yourself Against E-Illiteracy: Avoid Being Duped*, AM. BANKR. INST. J., Sept. 2004, *available at* http://www.kenwithers.com/articles/seward0904.pdf. Mr. Seward's article evoked a response from another commentator who stated that "deduplication" is not necessarily indicative of bad faith discovery and is often necessary. *See* George Socha, *Jack Seward's "Avoid Being Duped"—George Socha Responds*, Sept. 2004, http://www.kenwithers.com/articles/socha0904.html.

120. *See* COHEN & LENDER, *supra* note 4, app. 1A, at 1-38 to -39.

121. Under the Securities Exchange Act of 1934, companies in the securities trading industry must retain and keep e-mail correspondence readily accessible for a minimum of three years. 17 C.F.R. §§ 240.17a-3, 240.17a-4 (2006). In a recent announcement, EMC Corporation, an information storage and management firm, described its new archive and e-mail backup systems that automatically capture and index all e-mail messages, thereby allowing retrieval "within seconds rather than sorting through thousands of files." Press Release, EMC, EMC Helps Adirondack Electronics Markets Comply with SEC and NASD Regulations (June 7, 2004), *available at* http://www.emc.com/news/emc_releases/showRelease.jsp?id=2269.

122. Zubulake v. UBS Warburg LLC (*Zubulake I*), 217 F.R.D. 309 (S.D.N.Y. 2003).

is high and the required speed is very fast, i.e., milliseconds." Examples of online data include hard drives.

2. *Near-line data*: "This typically consists of a robotic storage device (robotic library) that houses removable media, uses robotic arms to access the media, and uses multiple read/write devices to store and retrieve records." Examples include optical disks.
3. *Offline storage/archives*: "This is removable optical disk or magnetic tape media, which can be labeled and stored in a shelf or rack. Off-line storage of electronic records is traditionally used for making disaster copies of records and also for records considered 'archival' in that their likelihood of retrieval is minimal. Accessibility to off-line media involves manual intervention and is much slower than on-line or near-line storage." The principled difference between nearline data and offline data is that offline data lacks "the coordinated control of an intelligent disk subsystem," and is, in the lingo, JBOD ("Just a Bunch of Disks").
4. *Backup tapes:* "A device, like a tape recorder, that reads data from and writes it onto a tape. Tape drives have data capacities of anywhere from a few hundred kilobytes to several gigabytes. Their transfer speeds also vary considerably . . . [.] The disadvantage of tape drives is that they are sequential-access devices, which means that to read any particular block of data, you need to read all the preceding blocks." As a result, "[t]he data on a backup tape are not organized for retrieval of individual documents or files [because] . . . the organization of the data mirrors the computer's structure, not the human records management structure." Backup tapes also typically employ some sort of data compression, permitting more data to be stored on each tape, but also making restoration more time-consuming and expensive, especially given the lack of uniform standard governing data compression.
5. *Erased, fragmented or damaged data*: "When a file is first created and saved, it is laid down on the [storage media] in contiguous clusters . . . [.] As files are erased, their clusters are made available again as free space. Eventually, some newly created files become larger than the remaining contiguous free space. These files are then broken up and randomly placed throughout the disk." Such broken-up files are said to be "fragmented," and along with damaged and

> erased data can only be accessed after significant processing.[123]

Judge Scheindlin noted that "the first three categories are typically identified as accessible, and the latter two as inaccessible."[124] The court further refined the distinction between inaccessible and accessible data by noting that accessible data "is stored in a readily usable format. . . . [It] does not need to be restored or otherwise manipulated to be usable."[125] In contrast, inaccessible data is not "readily usable" and must be restored, de-fragmented, or reconstructed before the data is usable.[126] This characterization of inaccessible data is therefore dependent on the format chosen for the data and the technology associated with that format choice. In essence, the owner of the data chooses when and how to make data inaccessible.[127]

The proposed amendments to the discovery rules under the Federal Rules of Civil Procedure cover this distinction between accessible and inaccessible data.[128] A proposed amendment to Rule 26(b)(2) provides that a party need not review or turn over inaccessible information unless an adversary moves for disclosure and shows good cause for the court to order the discovery. Under the new Rule 26(b)(2)(B),

> A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C).[129]

---

123. *Id.* at 318–19 (footnotes omitted).

124. *Id.* at 319–20.

125. *Id.* at 320.

126. *Id.*

127. *See* William R. Denny & Elizabeth J. King, *Electronic Discovery: Understanding Preservation Obligations, the Potential for Cost Shifting, and Current Developments*, POTTER ANDERSON & CORROON LLP (Nov. 2004), http://www.potteranderson.com/news-publications-0-102.html; *see also* Quinby v. WestLB AG, No. 04Civ.7406(WHP)(HBP), 2005 WL 3453908, at *8 n.10 (S.D.N.Y. Dec. 15, 2005) (declining to sanction the defendant for converting data from an accessible to an inaccessible format after becoming aware of the plaintiff's potential claim); *supra* text accompanying notes 95–101 (discussing the *Quinby* holding).

128. *See supra* note 20 and accompanying text. Additional updates and links to commentary on the proposed discovery rules can be found at the web site maintained by Ken Withers of the Federal Judicial Center. Electronic Discovery Rules, Proposed Rules, Commentary, & Debate, http://www.kenwithers.com/rulemaking/index.html (last visited Oct. 10, 2006).

129. JUDICIAL CONFERENCE REPORT, *supra* note 19, app. C, at 45–46. Under the renumbered rule, Rule 26(b)(2)(C) contains the proportionality limits that require the court to restrict otherwise permissible discovery methods if it finds that

Upon a request for disclosure, the responding party would have to show that the information was "not reasonably accessible because of undue burden or cost."[130] This standard of inaccessibility will vary according to the technology used, but "examples under current technology include deleted information, information kept on some backup-tape systems for disaster recovery purposes, and legacy data remaining from systems no longer in use."[131] The court can then require disclosure only for good cause and on specific terms and conditions. The procedure resembles the two-tier approach[132] that generally applies to disputed discovery in existing Federal Rule of Civil Procedure 26(b)(1). Although corporate counsel have generally applauded this two-tier approach for inaccessible information, some have criticized it as unnecessary and potentially confusing.[133] One commentator has noted, "Without more guidance—including concrete examples in the Commentary—as to what 'reasonably accessible' means, this rule should not be adopted. It threatens to give companies too much of an 'easy out'—an excuse not to offer the plaintiff all relevant records."[134] If a party does not have to produce inaccessible data, that inaccessible data might also be outside the scope of the duty to preserve.

The Advisory Committee attempted to address this concern in the committee notes to the proposed amendment when it stated, "A party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence."[135] This admonishment, however, is tempered with the comment that the preservation obligation will "depen[d] on the circumstances" and that one factor to consider would be "whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources."[136] Once a responding party has self-identified a source as not reasonably

---

> (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.

Id. app. C, at 46–47.

130. *Id.* app. C, at 46.

131. *Id.* at 30–31.

132. *See id.* at 31. "Lawyers sophisticated in these problems are developing a two-tier practice in which they first obtain and examine the information that can be provided from easily accessed sources and then determine whether it is necessary to search the difficult-to-access sources." *Id.*

133. *See* Mary P. Gallagher, *Federal Courts Propose Rules for E-Discovery*, N.J.L.J., Sept. 8, 2004; James E. Rooks, Jr., *Will E-Discovery Get Squeezed?*, TRIAL, Nov. 2004, at 20–22.

134. Anita Ramasastry, *The Proposed Federal E-Discovery Rules: While Trying to Add Clarity, the Rules Still Leave Uncertainty*, FINDLAW'S WRIT: LEGAL COMMENTARY, Sept. 15, 2004, http://writ.findlaw.com/ramasastry/20040915.html.

135. JUDICIAL CONFERENCE REPORT, *supra* note 19, app. C, at 48.

136. *Id.* app. C, at 87.

accessible, the party has no further duty (unless required by court order) to examine the contents of the inaccessible source. It is unclear how a responding party could ever show that it had a reasonable basis for believing that information was only available on an inaccessible source until the party had actually searched *accessible* sources first. If that is the case, it would seem that information on inaccessible sources would have to be preserved until the completion of discovery. Such a reading of Proposed Rule 26(b)(2) conflicts with Proposed Rule 37(f), which creates a safe harbor from sanctions if information is destroyed as a result of the routine operation of computer systems.[137] Indeed, the Judicial Conference noted, "Even when litigation is anticipated, it can be very difficult to interrupt or suspend the routine operation of computer systems to isolate and preserve discrete parts of the information they overwrite, delete, or update on an ongoing basis, without creating problems for the larger system."[138] Thus, the accessibility of electronic information is largely dependent on an organization's document retention and destruction policy.

C. *Document Retention and Destruction Policies and the Duty to Preserve Evidence*

Document retention policies are somewhat of a misnomer because, in addition to describing what and how information should be retained, these policies define when corporate records should be destroyed or, in the case of electronic records, recycled.[139] Organizational retention requirements are "self-defining: That is, companies operate in environments governed by legal and regulatory specifications that mandate the retention of certain records. Competitive and other business needs may likewise require that particular records be retained. Generally, it is up to the

---

137. *See infra* Part III.C.

138. JUDICIAL CONFERENCE REPORT, *supra* note 19, at 32.

139. A document retention policy has traditionally been defined as:

> [A] set of guidelines or rules governing storage and destruction of paper records. Such policies typically prescribe time periods during which certain types of documents should be retained, and provide that at the expiration of the prescribed time period the documents should be destroyed, perhaps by means specified in the policy.

COHEN & LENDER, *supra* note 4, § 4.01, at 4-3. The primary motivation for such a policy was space limitations. *Id.* Because storage of electronic documents has little cost (compared with paper storage), companies have been slow to implement retention policies for electronic documents. *See Poor Records Practices Are the Norm, Survey Finds*, TRANSFORM MAGAZINE, Apr. 1, 2004, *available at* http://www.transformmag.com/productbriefs/showArticle.jhtml?articleID=18311435. For sample document retention policies, see Policy and Procedure: Document Retention Procedures for Common Financial Transactions, Harvard University, http://vpf-web.harvard.edu/documents/actts_retention_1_23_01.html (last visited Oct. 10, 2006) and The Pew Charitable Trusts Document Retention Policy, Consortium of Foundation Libraries, http://www.foundationlibraries.org/Pew%20Trusts%20document%20policy.pdf (last visited Oct. 10, 2006).

company to determine what records fall into the latter category."[140] When it comes to electronic information and the duty to preserve evidence, many companies are struggling to determine the appropriate retention policy.

1. Retention Policies and the Management of Electronically Stored Information

Flawed information management policies may put electronic information at risk. The state of information management was explored in the Cohasset Survey, co-sponsored by the Association of Information and Image Management and the Association of Records Managers and Administrators.[141] The Cohasset Survey found that 43% of the organizations represented did not include digital records in their retention schedules,[142] and 49% of the respondent organizations had no formal e-mail retention policy.[143] Compared with earlier surveys, the respondents' view on the effectiveness of their document retention policies has improved.[144] The 2003 results showed that even when companies had a record retention policy that included electronic records, 38% of the respondents failed to follow their own schedules.[145] In 2005, this figure decreased significantly to 29%.[146] While the number of respondents expressing low levels of confidence in the accuracy and reliability of their electronic records has improved by 21% since 2003, 49%—almost half—of the respondents still came to a negative conclusion.[147] While the general progress is uplifting, the collective results continue to indicate that "with an organization's records being long recognized as its 'corporate memory,' [the] lack of awareness and preparation soon will manifest itself in 'Corporate Alzheimer's'—the old digital records exist on the storage media, but are not accessible due to hardware and/or software obsolescence."[148]

---

140. Brady & Cohen, *supra* note 26, at S4. One commentator suggests that a corporation implementing a document retention program should:

> (1) systematically develop the program; (2) adopt a program that covers all records, including reproductions; (3) include provisions for records maintained on other media; (4) identify appropriate procedures for obtaining written approvals for all records retention schedules; (5) strictly adhere to the policy that is instituted; (6) articulate appropriate control and management provisions; (7) provide for the suspension of document destruction where litigation is imminent; and (8) retain all documentation relating to the development and implementation of the program itself.

Cotton, *supra* note 26, at 422. The writer also argues that a reasonable retention period for electronic data should be longer because of the ease of storage. *Id.* at 429–30.

141. *See* COHASSET SURVEY, *supra* note 29 and accompanying text.

142. *See* COHASSET SURVEY, *supra* note 29, at 22.

143. *Id.* at 44.

144. *Id.* at 5.

145. *Id.* at 22–23.

146. *Id.*

147. *Id.* at 33–34.

148. *See id.* at 37.

2. Problems with Defining the Scope of the "Litigation Hold"

While business and legal requirements may guide an organization's information management policies, the prospect of litigation may alter these policies. As the court in *Zubulake IV* noted:

> [A]nyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary. "While a litigant is under no duty to keep or retain every document in its possession . . . it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request."[149]

This organizational duty to suspend its document management policies to preserve potentially relevant evidence is referred to as a litigation hold.[150] Within an organizational setting, however, it is often unclear what types of electronic information are actually subject to the litigation hold, especially with respect to backup tapes and e-mails.

For example, the court in *Zubulake IV* noted that as a general rule, a "litigation hold does not apply to inaccessible backup tapes."[151] However, if the backup tapes were "accessible (i.e., actively used for information retrieval), then such tapes *would* likely be subject to the litigation hold."[152] In addition, the court noted that if the company "can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of 'key players' to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available."[153] Thus, while the court excused a party from the duty to preserve *all* backup tapes, it clarified that *some* backup tapes may still be subject to a duty to preserve.[154] Both the technology used to create the backup

149. Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 217 (S.D.N.Y. 2003) (quoting Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 72 (S.D.N.Y. 1991)).

150. *Id.* at 218.

151. *Id.* A backup system periodically copies the contents of the company's computer systems to a series of tapes so that in the event of a catastrophic system failure, the company may restore its computer systems. The media used, typically individual magnetic tapes, are routinely recycled for reuse and are not intended for routine retrieval. Because their sole intended use is for the protection of the company's data in the event of a catastrophic computer failure, access to their contents is often difficult, time-consuming, and expensive.

152. *Id.*

153. *Id.*

154. *Id.*; *see also* Linnen v. A.H. Robins Co., 10 Mass. L. Rpt. 189, 193–95 (Super. Ct. 1999) (sanctioning the defendant for recycling and resulting destruction of e-mail backup tapes after an ex parte order was in effect requiring the defendant to preserve the evidence). The court in *Linnen* noted:

> While the court certainly recognizes the significant cost associated with restoring and producing responsive communications from these tapes . . . this is one of the risks taken on by companies which have made the decision to avail

tapes, and the manner in which backup tapes are catalogued and organized are solely within an organization's discretion. The ruling in *Zubulake IV* seems to suggest that an organization can avoid the duty to preserve backup tapes by using a disorganized system that renders some backup tapes inaccessible.

In addition to the limited, and somewhat unclear, duty of a company to preserve backup tapes, courts also limit the duty to preserve e-mail communications. In *Concord Boat Corp. v. Brunswick Corp.*,[155] the court excused the defendant's failure to preserve e-mails relevant to the action because such a preservation obligation would be too burdensome:

> [T]o hold that a corporation is under a duty to preserve all e-mail potentially relevant to any future litigation would be tantamount to holding that the corporation must preserve all e-mail. . . . Any corporation the size of Defendant (or even much smaller) is going to be frequently involved in numerous types of litigation. Whether it be patent, trademark, labor or antitrust suits, the threat of litigation is ever present for large, successful corporations. Arguably, most e-mails, excluding purely personal communications, could fall under the umbrella of "relevant to potential future litigation." . . . Thus, it would be necessary for a corporation to basically maintain all of its e-mail. Such a proposition is not justified.[156]

Thus, while not sanctioning prelitigation destruction of e-mail, the court did note that the defendant "had a duty to preserve relevant e-mails once the complaint was filed in th[e] case."[157] Therefore, an organization should carefully consider the business value, and if applicable, the regulatory requirements concerning retained e-mails, and if appropriate, maintain a relatively short retention schedule for e-mail communications to avoid sanctions.[158] Within an organizational setting, defining the boundaries of the duty to preserve evidence in anticipation of litigation will depend upon the organization's document retention and destruction policy and the technology it chooses to use to implement that policy.

3. *Compliance Issues During a Litigation Hold*

> themselves of the computer technology now available to the business world. To permit a corporation to reap the benefits of such technology and simultaneously use that technology as a shield in litigation would lead to incongruous and unfair results.

Id. at 192 (citation omitted).

155. No. LR-C-95-781, 1997 WL 33352759 (E.D. Ark. Aug. 29, 1997).

156. *Id.* at *4 (describing the costs associated with retaining all e-mails as "staggering").

157. *Id.* at *5.

158. *See, e.g.*, Broccoli v. Echostar Commc'ns Corp., 229 F.R.D. 506, 510, 512 (D. Md. 2005) (sanctioning a company for destroying e-mail records after notice of litigation, but noting that a twenty-one day recycling schedule for the irretrievable destruction of e-mails was a "risky but arguably defensible business practice undeserving of sanctions").

When litigation is threatened, the potential party must harmonize its document retention policy with the duty to preserve evidence. A duty to preserve evidence supersedes scheduled destruction under a document retention policy and mandates that relevant documents be subject to a litigation hold.[159] As described in *Zubulake IV*, "Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents."[160] For corporate officers and legal counsel, this "is not a passive obligation. Rather, it must be discharged actively . . . ."[161] Typically, corporate counsel (whether it be in-house or outside counsel) makes the initial determination when litigation is anticipated. Therefore, "the obligation to preserve evidence runs first to counsel, who then has a duty to advise and explain to the client its obligation to retain pertinent documents that may be relevant to the litigation."[162]

Although some decisions focus on the failure of senior management to assure compliance with a litigation hold,[163] several recent decisions have focused on the

---

159. Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 218 (S.D.N.Y. 2003); *see also* Danis v. USN Commc'ns, Inc., 53 Fed. R. Serv. 3d (West) 828, 878 (N.D. Ill. 2000) (sanctioning defendant for failure to create clear procedures and standards to ensure preservation of relevant documents); *In re* Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598, 615 (D.N.J. 1997) (requiring a litigant to create a "comprehensive document preservation plan" after a court order to preserve documents); Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 72 (S.D.N.Y. 1991) (describing litigants' duty to preserve documents relevant to litigation) (quoting William T. Thompson Co. v. Gen. Nutrition Corp., 593 F. Supp. 1443, 1455 (C.D. Cal. 1984))); *William T. Thompson*, 593 F. Supp. at 1448 (finding that a company's continuation of its informal document destruction procedures after an order to preserve relevant documents violated the company's obligation to retain and preserve such documents).

160. 220 F.R.D. at 218. Organizations may have difficulty determining at what point litigation is in fact anticipated. For example, when a company hired experts to implement a document retention policy so that the company would be "battle ready" for a litigation strategy to protect its intellectual property, two different courts looking at exactly the same facts arrived at polar opposite views concerning the document retention policy. *Compare* Hynix Semiconductor Inc. v. Rambus Inc., No. C-00-20905 RMW, 2006 WL 565893, at *22–24 (N.D. Cal. Jan. 5, 2006) (finding that litigation was not anticipated when document retention policy was implemented because several contingencies stood in the way of litigation, and the company had not yet budgeted for litigation), *with* Samsung Elecs. Co. v. Rambus Inc., No. Civ.A. 3:05CV406, 2006 WL 2038417, at *37–41 (E.D. Va. July 18, 2006) (specifically disagreeing with *Hynix* and finding that the document retention policy was an "integral part of its litigation strategy . . . [to] target for destruction documents that are discoverable in litigation").

161. *Danis*, 53 Fed. R. Serv. 3d (West) at 869.

162. Telecom Int'l Am., Ltd. v. AT&T Corp., 189 F.R.D. 76, 81 (S.D.N.Y. 1999), *aff'd*, 280 F.3d 175, 181 (2d Cir. 2001) (citing Kan.-Neb. Natural Gas Co. v. Marathon Oil Co., 109 F.R.D. 12, 18 (D. Neb. 1983)); *see also* N.Y. State Nat'l Org. for Women v. Cuomo, No. 93 Civ. 7146(RLC) JCF, 1998 WL 395320, at *2 (S.D.N.Y. July 14, 1998) (citing *Turner*, 142 F.R.D. at 73) (holding that counsel have a duty to advise their clients to take reasonable steps to preserve records subject to discovery); *Turner*, 142 F.R.D. at 73–74 ("[A] party's discovery obligations are not satisfied by relying on non-parties to preserve documents.") (citing Struthers Patent Corp. v. Nestle Co., 558 F. Supp. 747, 765 (D.N.J. 1981)).

163. United States *ex rel.* Koch v. Koch Indus., Inc., 197 F.R.D. 463, 484 (N.D. Okla. 1998) ("The obligation to preserve evidence that is potentially relevant to imminent or ongoing litigation is an affirmative duty that rests squarely on the shoulders of senior corporate officers."); *In re Prudential*, 169 F.R.D. at 615 ("The obligation to preserve documents that are potentially discoverable materials

attorney's responsibility to monitor compliance.[164] An attorney's responsibility concerning the preservation of evidence is described in ABA Civil Discovery Standard 10: "When a lawyer who has been retained to handle a matter learns that litigation is probable or has been commenced, the lawyer should inform the client of its duty to preserve potentially relevant documents in the client's custody or control and of the possible consequences of failing to do so."[165]

In *Zubulake V*, the court described the attorney's obligation to monitor compliance with an organizational client's duty to preserve electronic evidence.[166] The attorney's obligations begin with the instruction to the client that a litigation hold is necessary.[167] In addition to describing the subject matter of the anticipated litigation, the attorney should inform the client of the full range of potential negative consequences that could result from the destruction of evidence, including contempt of court, civil and criminal penalties and sanctions, default judgment, or dismissal.[168] At that point, counsel must supervise compliance with the litigation hold and monitor the client's efforts to retain and produce any relevant documents. The critical factor in fulfilling this obligation is the quality of the communication between client and attorney.[169] As noted in the Cohassett Survey, because many companies fail even to include digital information or e-mail within their document retention policies,[170] it is imperative that an attorney apprise corporate clients of the need to locate and preserve potentially relevant information from electronic sources as well as traditional paper sources. Thus, it is incumbent upon an attorney to understand a corporate client's document retention policy, along with its "data retention architecture."[171] To safeguard electronic sources of information, the

---

is an affirmative one that rests squarely on the shoulders of senior corporate officers.").

164. Zubulake v. UBS Warburg LLC (*Zubulake V*), 229 F.R.D. 422, 432–34 (S.D.N.Y. 2004); *see also* Metro. Opera Ass'n v. Local 100, Hotel Employees & Rest. Employees Int'l Union, 212 F.R.D. 178, 221–24 (S.D.N.Y. 2003) (ordering a default judgment as a discovery sanction based primarily on counsel's failure to adequately notify and supervise the client concerning its preservation obligations).

165. AM. BAR ASS'N, CIVIL DISCOVERY STANDARDS, *supra* note 74, Standard 10, at 20. Standard 29(a)(i) is "designed to provide a checklist to assist counsel in identifying types of electronic data as to which the duty to preserve may apply, once that duty has been triggered under applicable law." AM. BAR ASS'N, CIVIL DISCOVERY STANDARDS, *supra* note 74, Standard 29(a) cmt. (a)(i), at 61. Moreover, the Model Rules of Professional Conduct also support an attorney's obligation to preserve evidence, stating that "[a] lawyer shall not . . . unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value [and] . . . shall not counsel or assist another person to do any such act. . . ." MODEL RULES OF PROF'L CONDUCT R. 3.4(a) (2004).

166. *Zubulake V*, 229 F.R.D. at 431–34.

167. *Id.* at 432.

168. N.Y. State Nat'l Org. For Women v. Cuomo, No. 93 Civ. 7146(RLC) JCF, 1998 WL 395320, at *2 (S.D.N.Y. July 14, 1998) (noting that failing to instruct the defendant to retain documents after service of the complaint, but before specific document requests, could expose counsel to sanctions).

169. *Zubulake V*, 229 F.R.D. at 432 ("Proper communication between a party and her lawyer will ensure (1) that all relevant information (or at least all sources of relevant information) is discovered, (2) that relevant information is retained on a continuing basis; and (3) that relevant non-privileged material is produced to the opposing party.").

170. COHASSET SURVEY, *supra* note 29, at 20–23.

171. *Zubulake V*, 229 F.R.D. at 432.

corporate attorney must confer with information technology personnel to learn about the "system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm's recycling policy."[172] Unfortunately, this preliminary step is often filled with the risk of miscommunication due to of the lack of preparedness that many companies have for a litigation hold.[173]

In addition to conferring with the information technology personnel, corporate counsel should identify the key players in the anticipated litigation and communicate directly with them concerning their use of digital sources.[174] The standard described in *Zubulake V* is much more than mere notice of the litigation hold; corporate counsel must engage in "affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched."[175] Because there is a "duty to supplement" discovery responses under Rule 26 of the Federal Rules of Civil Procedure, corporate counsel has a continuing duty to monitor compliance and ensure preservation obligations are being met.[176] The court in *Zubulake V*, however, noted that this obligation had its limits:

> [T]he requirement must be reasonable. A lawyer cannot be obliged to monitor her client like a parent watching a child. At some point, the client must bear responsibility for a failure to

---

172. *Id.* The Cohasset Survey found that more than three-fifths (61%) of the respondents reported that information systems/technology departments had primary responsibility for the day-to-day management of their organization's electronic records. COHASSET SURVEY, *supra* note 29, at 28. Because of the importance of records management in an increasingly electronic environment, the Cohasset Survey concluded that "records management professionals need to both proactively evolve their roles and responsibilities as well as concurrently acquire the skill sets necessary to win the increasingly important position of leading an organization's records management program." *Id.* at 32.

173. COHASSET SURVEY, *supra* note 29, at 25 (stating that "[i]n 2005, just 57% of the survey respondents stated their organizations had a discovery request response plan"). These numbers were "astounding" to the study's authors, "given the degree of recent national media coverage on the issue of illegal document destruction and the substantive growth in the number of court-ordered records hold orders issued in the 1999–2003 period." *Id.* at 26. Further, "[p]rojecting this finding against the 2005 survey's universe of an estimated 10,000, 4,300 organizations do not have a formal hold order system in place." *Id. See* United States *ex rel.* Koch v. Koch Indus., Inc., 197 F.R.D. 463, 484 (N.D. Okla. 1998) (noting that despite imminent litigation, senior management failed to involve data processing managers and tape librarians in the preservation obligation or even provide any specific instructions as to what should be preserved in connection with the litigation).

174. *Zubulake V*, 229 F.R.D. at 432 ("Unless counsel interviews each [key] employee, it is impossible to determine whether all potential sources of information have been inspected."). The court recognized that it may not be possible for counsel to interview every key player, but counsel should, at a minimum, develop a system-wide keyword search of electronic sources and preserve a copy of each "hit." *Id.* In fact, information management companies are quickly developing information management systems that make the strategy described in *Zubulake V* quite feasible.

175. *Id.*

176. FED. R. CIV. P. 26(e)(1). As the Advisory Committee's notes to Rule 26(e) explain although the duty to supplement is nominally the party's, the lawyer is in the best position to "understand the significance" of discovery responses and to know when an update is needed. FED. R. CIV. P. 26(e) advisory committe's notes (1970). "In practice, therefore, the lawyer under a continuing burden must periodically recheck all interrogatories and canvass all new information." FED. R. CIV. P. 26(e) advisory committee's notes (1970); *see also Zubulake V*, 229 F.R.D. at 433.

> preserve. At the same time, counsel is more conscious of the contours of the preservation obligation; a party cannot reasonably be trusted to receive the "litigation hold" instruction once and to fully comply with it without the active supervision of counsel.[177]

Thus, the court in *Zubulake V* outlined the reasonable steps that counsel is expected to take to ensure compliance with the preservation obligation. First, counsel is responsible for issuing the initial litigation hold to the corporate entity and for periodically reissuing the preservation notice so that all employees, including new employees, are aware of their ongoing preservation obligation.[178] Second, counsel should engage in a clear dialogue with key players in the litigation to ensure that these employees specifically understand their preservation duty and how it applies to digital sources of information.[179] As with the litigation hold notice, periodic reminders should be reissued to these key players.[180] Finally, the court suggested that counsel take an active role in the collection and maintenance of potentially relevant digital information:

> [C]ounsel should instruct all employees to produce electronic copies of their relevant active files. Counsel must also make sure that all backup media which the party is required to retain is identified and stored in a safe place. In cases involving a small number of relevant backup tapes, counsel might be advised to take physical possession of backup tapes. In other cases, it might make sense for relevant backup tapes to be segregated and placed in storage.... By taking possession of, or otherwise safeguarding, all potentially relevant backup tapes, counsel eliminates the possibility that such tapes will be inadvertently recycled.[181]

The reasonableness of these suggested steps, particularly the last step, will most likely be a continuing source of litigation.

The difficulties encountered when counsel and senior management attempt to coordinate preservation obligations are well documented.[182] Although the court in

---

177. 229 F.R.D.at 433 (citing Telecom Int'l Am., Ltd. v. AT&T Corp., 189 F.R.D. 76, 81 (S.D.N.Y. 1999), *aff'd*, 280 F.3d 175, 181 (2d Cir. 2001)).

178. *Id.*

179. *Id.* at 433–34.

180. *Id.* at 434.

181. *Id.*

182. *See, e.g.*, Metro. Opera Ass'n v. Local 100, Hotel Employees and Rest. Employees Int'l Union, 212 F.R.D. 178, 209–15 (S.D.N.Y. 2003) (describing in detail the lack of oversight counsel had in monitoring the client's duty to preserve and produce electronic evidence); GTFM, Inc. v. Wal-Mart Stores, Inc., 49 Fed. R. Serv. 3d (West) 219, 222 (S.D.N.Y. 2000) (sanctioning the defendant for failure to preserve and produce evidence in part due to counsel's inadequate inquiries into defendant's computer capacity); N.Y. State Nat'l Org. for Women v. Cuomo, No. 93 Civ. 7146(RLC)JCF, 1998 WL 395320, at *2 (S.D.N.Y. July 14, 1998) (noting counsel's duty to advise the client of pending litigation and the requirement to preserve potentially relevant evidence).

the *Zubulake* litigation found that the defendant's in-house and outside counsel had frequently advised UBS of its preservation obligations, the court also found that counsel failed to adequately communicate with all key players by not communicating the litigation hold instructions to the human resources employee most involved with Zubulake's termination.[183] Moreover, even with respect to the key players with whom counsel *did* communicate, the court found a failure to "ascertain each of the key players' document management habits."[184] Although the court acknowledged the defendant's counsel could have done more, the court also found that UBS deleted information it knew it should have preserved "in defiance of explicit instructions not to."[185]

In fact, senior management also has an affirmative duty to implement the litigation hold and, if necessary, to coordinate the litigation hold with any existing document retention policy.[186] Moreover, senior management is charged with communicating preservation obligations with employees. "[M]anagement cannot shield a corporation from responsibility because an employee routinely destroyed information relevant to imminent or ongoing litigation."[187] When senior management has failed in their affirmative duty to communicate the duty to preserve information relevant to anticipated or existing litigation, courts have often levied fines against both the company and individual managers.[188]

Despite the obligations imposed upon lawyers and their clients to preserve information potentially relevant to anticipated or actual litigation, when electronic information is destroyed, the number of acceptable extenuating circumstances

---

183. Zubulake v. UBS Warburg LLC (*Zubulake V*), 229 F.R.D. 422, 435 (S.D.N.Y. 2004).

184. *Id.* at 436.

185. *Id.*

186. *See, e.g.*, Bradley v. Sunbeam Corp., No. Civ.A 5:99CV144, 2003 WL 21982038, at *13 (N.D. W. Va. Aug. 4, 2003) (finding that senior management has the responsibility to request suspension of the company's product destruction process when faced with litigation), *vacated and rev'd on other grounds*, 378 F.3d 373 (4th Cir. 2004).

187. United States *ex rel.* Koch v. Koch Indus., Inc., 197 F.R.D. 463, 484 (N.D. Okla. 1998) (finding that senior management failed to meet its preservation obligations when there was no policy or procedure for notifying employees of anticipated litigation and the associated need for employees to preserve evidence); *see also* Diersen v. Walker, No. 00 C 2437, 2003 WL 21317276, at *5 (N.D. Ill. June 6, 2003) (finding that a party's failure to warn its employees to preserve potentially relevant documents showed a disregard of the duty to preserve evidence).

188. *See, e.g.*, United States v. Philip Morris USA, Inc., 327 F. Supp. 2d 21, 26 n.1 (D.D.C. 2004) (fining eleven of the defendant's corporate managers $250,000 each for the destruction of relevant e-mails after a preservation order had specifically required the preservation of those e-mails); Danis v. USN Commc'ns, Inc., 53 Fed. R. Serv. 3d (West) 828, 899 (N.D. Ill. 2000) (fining the CEO of the defendant company $10,000 for failing to preserve information on a computer database); Procter & Gamble Co. v. Haugen, 179 F.R.D. 622, 632 (D. Utah 1998) (fining senior P&G management $10,000 for failing to save e-mail communications from individuals that P&G had specifically identified as having knowledge of the issues in the litigation); *In re* Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598, 617 (D.N.J. 1997) (fining the company $1 million for the failure of senior management to implement a comprehensive preservation order and communicate that policy to employees despite the existence of a preservation order in the action). As discussed in Part III, whether a preservation order is in effect has a significant impact on the degree of punishment that is levied against senior management for the destruction of electronic information subject to the preservation duty.

surrounding the destruction seems to be growing. While a few major cases might suggest that the destruction of electronic information subject to a preservation obligation might lead to onerous sanctions, the developing jurisprudence suggests a far different scenario.

III. CONSEQUENCES FOR FAILING TO OBSERVE THE DUTY TO PRESERVE

The American justice system is premised on the fair adjudication of disputes through both sides obtaining and presenting the relevant evidence.[189] When one side learns that evidence has been destroyed despite a duty to preserve that evidence, a motion for sanctions is the common response.[190] The imposition of sanctions for the destruction of evidence is within the trial court's discretion and is based on the court's "inherent power to regulate litigation, preserve and protect the integrity of proceedings before it, [] sanction parties for abusive practices," and on Federal Rule of Civil Procedure 37.[191] The most frequent sanctions for the destruction of evidence include fines[192] and adverse inference jury instructions;[193] however, in especially egregious cases, the court may end the litigation.[194]

A party can be sanctioned for the destruction of evidence only if it first had a duty to preserve it.[195] As discussed in Part II, whether the duty to preserve exists depends on an analysis of when the duty first attached to the information and the

---

189. As the court in *Danis* noted:

> This fair opportunity to be heard is achieved through lawyers for each side, having obtained and marshaled the relevant evidence, presenting their clients' respective positions vigorously. Our system is premised on the view that through this clash of competing stories, judges and juries will have the information they need to make a fair decision. In our system of civil litigation, the discovery process is the principal means by which lawyers and parties assemble the facts, and decide what information to present at trial.
>
> . . . .
>
> . . . Parties and attorneys frequently are called upon to preserve and produce documents that are against their interest in a particular case. And when they do so, the parties and the attorneys uphold the integrity of our litigation system and inspire confidence in it.

Danis, 53 Fed. R. Serv. 3d (West) at 828–29.

190. *See* FED. R. CIV. P. 37(a)(4) (enabling a court to punish the litigant who did not adequately respond to an opposing party's discovery requests or to the court's orders compelling discovery). Even when destruction has taken place before the initiation of a lawsuit or the filing of a discovery request, courts have the inherent authority to sanction the offending party. *See* Capellupo v. FMC Corp., 126 F.R.D. 545, 550 (D. Minn. 1989).

191. *Capellupo*, 126 F.R.D. at 551 & n.14.

192. *See Philip Morris*, 327 F. Supp. 2d at 26 (fining the defendants a total of $2.75 million for the destruction of evidence).

193. *See* Zubulake v. UBS Warburg LLC (*Zubulake V*), 229 F.R.D. 422, 437 (S.D.N.Y. 2004) (granting the plaintiff an instruction to the jury that it could infer the destroyed evidence was adverse to the defendant).

194. *See* Telectron, Inc. v. Overhead Door Corp., 116 F.R.D. 107, 130 (S.D. Fla. 1987) (entering default judgment against defendant for wilful and bad faith document destruction).

195. Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 216 (S.D.N.Y. 2003). *See supra* Part II.A.1 (explaining when the duty to preserve is triggered).

scope of the duty.[196] However, merely finding a duty to preserve evidence is only the first step. To determine whether sanctions are warranted, federal courts generally follow the three part test outlined in *Schmid v. Milwaukee Electric Tool Corp.*:[197]

> (1) [T]he degree of fault of the party who altered or destroyed the evidence; (2) the degree of prejudice suffered by the opposing party; and (3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party and, where the offending party is seriously at fault, will serve to deter such conduct by others in the future.[198]

In applying these factors, courts often require "that the records were destroyed with a 'culpable state of mind' and . . . that the destroyed evidence was 'relevant' to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense."[199] The destruction of electronic evidence poses significant challenges for both of these inquiries. When there is so much confusion about the nature of electronic information and its sources, at what point does the destruction of electronic evidence evince the requisite level of culpability? When the destruction of electronic evidence often entails the destruction of an entire source of information, how can the court judge the source's relevance to the litigation? As courts grapple with these and other questions, uncertainty about a party's obligations to preserve electronic evidence increases. Because of this uncertainty and the likelihood of avoiding sanctions, the viability of electronic evidence becomes precarious.

---

196. *Zubulake IV*, 220 F.R.D. at 216.

197. 13 F.3d 76 (3d Cir. 1994).

198. *Id.* at 79. Courts using the *Schmid* factors to determine sanctions for the destruction of evidence include: Advantacare Health Partners, LP v. Access IV, No. C 03-04496 JF, 2004 WL 1837997, at *4 (N.D. Cal. Aug. 17, 2004); Williams v. Am. Surplus, Inc., No. Civ.A. 02-7655, 2003 WL 22232882, at *2 (E.D. Pa. Aug. 4, 2003). However, some courts use a five factor test instead: "(1) whether the defendant was prejudiced [by the destruction of evidence]; (2) whether the prejudice can be cured; (3) the practical importance of the evidence; (4) whether the plaintiff['s destruction] was in good or bad faith; and (5) the potential for abuse if the evidence is not excluded" or the party is not otherwise sanctioned. Lewis v. Darce Towing Co., 94 F.R.D. 262, 266–67 (W.D. La. 1982).

199. *Zubulake IV*, 220 F.R.D. at 220 (quoting Byrnie v. Town of Cromwell, Bd. of Educ., 243 F.3d 93, 109 (2d Cir. 2001)); *see also* Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108 (2d Cir. 2002) (finding that the defendant's state of mind and the relevance to the plaintiff's claims were important factors in evaluating claims); Trigon Ins. Co. v. United States, 204 F.R.D. 277, 288 (E.D. Va. 2001) (stating that "assessment of sanctions depends most significantly on the blameworthiness of the offending party and the prejudice suffered by the opposing party"). As explained in *Zubulake V*, these two inquiries may be combined under some circumstances. "When evidence is destroyed in bad faith (i.e., intentionally or willfully), that fact alone is sufficient to demonstrate relevance. By contrast, when the destruction is negligent, relevance must be proven by the party seeking the sanctions." Zubulake v. UBS Warburg LLC (*Zubulake V*), 229 F.R.D. 422, 431 (S.D.N.Y. 2004) (citing *Residential Funding*, 306 F.3d at 109).

A. Determining Culpability for the Destruction of Digital Data

In determining the appropriate sanction, the level of culpability is of prime importance. When a party seeks a sanction that would end the litigation, such as requesting a dismissal or a default judgment, courts generally agree that the level of culpability must rise to the level of bad faith or willful destruction.[200] In contrast, when an adverse inference jury instruction is sought, especially within the context of destruction under a document retention policy, the circuits are split as to the level of required culpability.[201] The difference in the level of culpability required and the inconsistent evaluation of facts that satisfy the specified level of culpability combine to create an uncertainty in the law. While the proposed new discovery rules are intended to address this uncertainty, the new safe harbor in Rule 37 of the Federal Rules of Civil Procedure[202] may only serve to further weaken the viability of electronic evidence.

1. Termination of the Action with Clear Showing of Bad Faith

Some litigation conduct concerning the destruction of evidence subject to the duty to preserve is so clearly egregious that a sanction will be awarded based solely on the bad faith of the party. "Deliberate, willful and contumacious disregard of the judicial process and the rights of opposing parties justifies the most severe sanction[.]"[203] To establish this level of culpability, courts have applied a clear and convincing evidence standard to Rule 37 cases.[204] The plaintiffs met this standard in *Carlucci* when, together with other discovery misconduct, they successfully showed that the defendant "purge[d]" department files of all flight records that might be detrimental to the defendant in a law suit.[205] Similarly, in *Telectron v. Overhead Door Corp.*,[206] a default judgment was an appropriate sanction when an inexperienced in-house counsel "ordered the immediate destruction of documents directly pertaining to Plaintiff's Complaint and Request for Production, on the very day that these papers were served personally upon him."[207] The court found counsel's behavior to be "a willful and intentional attempt to place documentation

200. *See* Telectron, Inc. v. Overhead Door Corp., 116 F.R.D. 107, 131 (S.D. Fla. 1987); Carlucci v. Piper Aircraft Corp., 102 F.R.D. 472, 486 (S.D. Fla. 1984).

201. See cases cited *infra* note 219.

202. JUDICIAL CONFERENCE REPORT, *supra* note 19, app. C, at 86.

203. *Carlucci*, 102 F.R.D. at 486 (citing Nat'l Hockey League v. Metro. Hockey Club, 427 U.S. 639, 643 (1975)).

204. *See* Danis v. USN Commc'ns, Inc., 53 Fed. R. Serv. 3d (West) 828, 873 (N.D. Ill. 2000) (finding that the clear and convincing standard was most appropriate because sanctions resulting in the dismissal of the action should have the same stringent standard as required for a finding of contempt).

205. *Carlucci*, 102 F.R.D. at 481–86.

206. 116 F.R.D. 107 (S.D. Fla. 1987).

207. *Id.* at 109.

which he anticipated to be damaging to [the defendant's] interests in this litigation forever beyond the reach of Telectron's counsel."[208]

Parties have also met the clear and convincing standard by showing the willful destruction of electronic data. In *Computer Associates International, Inc. v. American Fundware, Inc.*,[209] the court granted a default judgment sanction in a copyright infringement case when the defendant intentionally destroyed computer source code even after a request for production and motion to compel.[210] In *Computer Associates*, the court stressed the sanction's dual purpose of punishment and deterrence:

> [I]t is well to remind litigants that such conduct will not be tolerated in judicial proceedings. Destruction of evidence cannot be countenanced in a justice system whose goal is to find the truth through honest and orderly production of evidence under established discovery rules. I hold that nothing less than default judgment on the issue of liability will suffice to both punish this defendant and deter others similarly tempted.[211]

Similarly, the court awarded the plaintiff a default judgment when the defendant, assisted by an unidentified relative, destroyed his laptop computer, burned his business records, and deposited the remains in the garbage where they were taken to the city dump.[212]

Yet in several cases where a party used software or other techniques specifically designed to delete or erase hard drives, courts have ordered lesser sanctions.[213] Although decided within the context of a criminal prosecution under

---

208. *Id.* at 109–10. Interestingly, when another inexperienced in-house counsel failed to preserve documents, the court fined the CEO $10,000 for delegating the preservation obligation to an unqualified employee. *Danis*, 53 Fed. R. Serv. 3d (West) at 845–47, 899.

209. 133 F.R.D. 166 (D. Colo. 1990).

210. *Id.* at 169–70.

211. *Id.* at 170.

212. Century ML-Cable Corp. v. Conjugal P'ship, 43 F. Supp. 2d 176, 180, 185 (D.P.R. 1998).

213. *See* Minn. Mining & Mfg. Co. v. Pribyl, 259 F.3d 587, 606 n.5 (7th Cir. 2001) (affirming an adverse inference jury instruction when one of the defendants destroyed evidence by downloading six gigabytes of music onto his laptop the night before he was supposed to turn his laptop over for a discovery request); Anderson v. Crossroads Capital Partners, No. Civ.01-2000 ADM/SRN, 2004 WL 256512, at *8 (D. Minn. Feb. 10, 2004) (finding that the plaintiff's recent installment and use of "CyberScrub," a commercially available file-wiping program, was not conduct so egregious as to merit dismissal, but instead warranted an adverse inference jury instruction); Kucala Enters., Ltd. v. Auto Wax Co., 57 Fed. R. Serv. 3d (West) 501, 509 (N.D. Ill. 2003) (rejecting the magistrate's recommendation that plaintiff's complaint be dismissed when the plaintiff used "Evidence Eliminator," a commercially available disk-wiping software, to "clean" approximately 15,000 files the night before a scheduled inspection, but upheld an award of expenses flowing from the discovery misconduct). Admittedly, sometimes computers just have bad luck, such as the computer that was struck by a falling air compressor, hit by its owner on several occasions to get it to operate, fell off the desk on "at least four to five occasions," and finally was dropped on the ground as the defendant arrived at the opposing counsel's office for a deposition. Ill. Tool Works, Inc. v. Metro Mark Prods., Ltd., 43 F. Supp. 2d 951, 955–56 (N.D. Ill. 1999). The court awarded the plaintiff its fees and costs to retrieve data from the

a federal obstruction of justice statute, *Arthur Andersen LLP v. United States*,[214] a recent unanimous Supreme Court decision, reversed the lower court's ruling involving the destruction of evidence under a document retention policy.[215] The Court held that the jury instructions used were flawed because they had "simply failed to convey the requisite consciousness of wrongdoing."[216] Thus, in some cases, despite a clear intent to destroy electronic evidence that the party knew was relevant to the litigation, courts do not see such conduct as rising to the level of culpability to warrant the most severe sanctions—the termination of the litigation. Instead, courts increasingly rely on a lesser sanction—the adverse inference instruction.

2. *Conflicting Standards of Culpability for Sanction of Adverse Inference Instruction*

The adverse inference instruction for the destruction of evidence is steeped in tradition and is "supported by evidentiary, prophylactic, punitive, and remedial rationales."[217] When a jury is given an adverse inference instruction, the jury is permitted, but not required, to assume that the destroyed evidence would have been unfavorable to the party responsible for its destruction.[218] In determining whether the inference should be awarded, a key consideration is the level of culpability of the party responsible for the destruction. Courts, however, are divided as to the

---

defendant's unlucky computer. *Id.* at 962.

214. 544 U.S. 696 (2005).

215. *Id.* at 698.

216. *Id.* at 706. Although the *Andersen* decision is limited to its facts, and Congress amended the statute involved after the prosecution was brought, the decision still signals a sympathetic view toward information management and the high level of culpability needed to find actionable wrongdoing. *See* Jonathan M. Redgrave et al., *Looking Beyond Arthur Andersen: The Impact on Corporate Records and Information Management Policies and Practices*, 52 FED. LAW., Sept. 2005, at 32, 34–36; *see also* Hamre v. Mizra, No. 02Civ.9088(PKL)(HBP), 2005 WL 1083978, at *2–3 (S.D.N.Y. May 9, 2005) (denying sanctions for the destruction of medical records evidence because "temporal coincidence" of the destruction was not enough to show bad faith).

217. Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998). The court in *Kronisch* also noted that the principle that an adverse inference is warranted against a party responsible for the loss or destruction of evidence is based on the famous common law case of *Armory v. Delamirie*. *Id.* at 126 n.11 (citing Armory v. Delamirie, (1722) 93 Eng. Rep. 664, 664 (K.B.)). In *Armory*, a chimney sweep who found a jewel sued a jeweler for the loss of the jewel and was entitled, based on the jeweler's return of the ring without the stone, to an inference that the stone was "of the finest water." *Armory*, 93 Eng. Rep. at 664; *see* Welsh v. United States, 844 F.2d 1239, 1246 (6th Cir. 1988) (discussing the origins of the spoliation inference). *See generally* Drew D. Dropkin, Note, *Linking the Culpability and Circumstantial Evidence Requirements for the Spoliation Inference*, 51 DUKE L.J. 1803, 1814 n.59 (2002) (quoting KOESEL & TURNBULL, *supra* note 10, at xiii) ("In issuing this adverse inference instruction to the jury, the chief justice in *Armory* also announced the legal maxim that would forever be associated with the spoliation inference: '*contra spoliatorem omnia praesumuntur*'—'All things are presumed against the spoliator.'").

218. *Kronisch*, 150 F.3d at 126; *see also* Zubulake v. UBS Warburg LLC (*Zubulake V*), 229 F.R.D. 422, 437 (S.D.N.Y. 2004) (granting an adverse inference instruction concerning willfully deleted e-mails); Linnen v. A.H. Robins Co., 10 Mass. L. Rpt. 189, 195 (Super. Ct. 1999) (awarding an adverse inference instruction for the destruction of backup tapes).

requisite level of culpability, particularly when the destruction occurs as a result of a document retention policy.[219]

In the landmark case of *Lewy v. Remington Arms Co.*,[220] the court addressed destruction of evidence under a document retention policy and whether an adverse inference instruction was appropriate.[221] This products liability action involved the safety features of a rifle, and the plaintiff had requested an adverse inference instruction because of the defendant's destruction of prior complaints and gun examination reports under its document retention policy.[222] The court remanded the case to the trial court and provided the following factors to determine whether destruction of evidence under a document retention policy warranted an adverse inference sanction: (1) whether the company's document retention policy "is reasonable considering the facts and circumstances surrounding the relevant documents;"[223] (2) "whether lawsuits concerning the complaint or related complaints have been filed, the frequency of such complaints, and the magnitude of the complaints;"[224] and (3) "whether the document retention policy was instituted in bad faith."[225] In defining what the court meant by "bad faith," the court explained that "if the corporation *knew or should have known* that the documents would become material at some point in the future then such documents should have been preserved. Thus, a corporation cannot blindly destroy documents and expect to be

---

219. Cases have required a clear showing of bad faith before sanctions, including an adverse inference instruction, could be imposed. Morris v. Union Pac. R.R., 373 F.3d 896, 901 (8th Cir. 2004) (citing Stevenson v. Union Pac. R.R., 354 F.3d 739, 746–48 (8th Cir. 2004)); Koons v. Aventis Pharms., Inc., 367 F.3d 768, 780 (8th Cir. 2004) (citing *Stevenson*, 354 F.3d at 746–48)); *Stevenson*, 354 F.3d at 746–47 (citing Lewy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988)); Wiginton v. CB Richard Ellis, Inc. (*Wiginton I*) No. 02 C 6832, 2003 WL 22439865, at *7 (N.D. Ill. Oct. 27, 2003) (citing Mathis v. John Morden Buick, Inc., 136 F.3d 1153, 1155 (7th Cir. 1998)); United States v. Taber Extrusions L.P., No. 4:00CV00255WRW, 2001 WL 1941318, at *2 (E.D. Ark. Dec. 27, 2001) (citing *Lewy*, 836 F.2d at 1112); Anderson v. Prod. Mgmt. Corp., No. Civ.A.98-2234, 2000 WL 492095, at *4 (E.D. La. Apr. 25, 2000) (citing Vick v. Tex. Employment Comm'n, 514 F.2d 734, 737 (5th Cir. 1975)); United States *ex rel* Koch v. Koch Indus., Inc., 197 F.R.D. 463, 486 (N.D. Okla. 1998). Other jurisdictions allow a lesser standard of culpability, including negligence. *See* Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108 (2d Cir. 2002) (citing Byrnie v. Town of Cromwell, Bd. of Educ., 243 F.3d 93, 109 (2d Cir. 2001)); Pace v. Nat'l R.R. Passenger Corp., 291 F. Supp. 2d 93, 99 (D. Conn. 2003) (citing *Residential Funding*, 306 F.3d at 108); Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 221 (S.D.N.Y. 2003); Shaffer v. RWP Group, Inc., 169 F.R.D. 19, 26 (E.D.N.Y. 1996); Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 75 (S.D.N.Y. 1991).

220. 836 F.2d 1104 (8th Cir. 1988).

221. *Id.* at 1109.

222. *Id.* at 1111.

223. *Id.* at 1112. The United States Supreme Court recently noted the acceptance of document retention policies:

> "Document retention policies," which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business. It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.

Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005) (citation omitted).

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

225. *Id.* (citing Gumbs v. Int'l Harvester, Inc., 718 F.2d 88, 96 (3d Cir. 1983)).

shielded by a seemingly innocuous document retention policy."[226] In 2004, the Eighth Circuit clarified the bad faith requirement of the *Lewy* decision, concluding:

> We have never approved of giving an adverse inference instruction on the basis of prelitigation destruction of evidence through a routine document retention policy on the basis of negligence alone. Where a routine document retention policy has been followed in this context, we now clarify that there must be some indication of an intent to destroy the evidence for the purpose of obstructing or suppressing the truth in order to impose the sanction of an adverse inference instruction.[227]

Requiring a more stringent standard of culpability when destruction occurs under a document retention policy makes it easier for companies to avoid sanctions.[228]

In contrast to the bad faith requirement for an adverse inference instruction followed in some courts, other jurisdictions have imposed the adverse inference sanction based on negligent conduct.[229] As explained in *Turner*, the remedial purpose of the sanction is furthered when the sanction is also available in the face of negligent conduct: "It makes little difference to the party victimized by the destruction of evidence whether that act was done willfully or negligently. The adverse inference provides the necessary mechanism for restoring the evidentiary balance."[230] However, even when courts are willing to accept a negligence level of culpability, the courts continue with their analysis to consider the relevance of the

---

226. *Id.* (emphasis added).

227. Stevenson v. Union Pac. R.R., 354 F.3d 739, 747 (8th Cir. 2004) (citing *Lewy*, 836 F.2d at 1112).

228. *See* Morris v. Union Pac. R.R., 373 F.3d 896, 899–902 (8th Cir. 2004) (citing *Stevenson*, 354 F.3d at 747–48); Koons v. Aventis Pharms., Inc., 367 F.3d 768, 780 (8th Cir. 2004) (citing *Stevenson*, 354 F.3d at 746–47); *Stevenson*, 354 F.3d at 747; Park v. City of Chicago, 297 F.3d 606, 615 (7th Cir. 2002) (citing Rummery v. Ill. Bell Tel. Co., 350 F.3d 553, 558–59 (7th Cir. 2001)); Diersen v. Walker, No. 00 C 2437, 2003 WL 21317276, at *5 (N.D. Ill. June 6, 2003); United States v. Taber Extrusions L.P., No. 4:00CV00255WRW, 2001 WL 1941318, at *2–3 (E.D. Ark. Dec. 27, 2001); Anderson v. Prod. Mgmt. Corp., No. Civ.A.98-2234, 2000 WL 492095, at *4 (E.D. La. Apr. 25, 2000) (citing Vick v. Tex. Employment Comm'n, 514 F.2d 734, 737 (5th Cir. 1975)).

229. *See* Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108 (2d Cir. 2002); Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 220 (S.D.N.Y. 2003) (citing *Residential Funding*, 306 F.3d at 108); Trigon Ins. Co. v. United States, 204 F.R.D. 277, 286 (E.D. Va. 2001) (stating that "proof of bad faith is not necessary to obtain relief from spoliation"); Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 75–76 (S.D.N.Y. 1991). Further, another court has suggested other remedies for negligent conduct, including admitting disputed facts against the offending party. *See* Pressey v. Patterson, 898 F.2d 1018, 1024 (5th Cir. 1990).

230. *Turner*, 142 F.R.D. at 75 ("The inference is *adverse* to the destroyer not because of any finding of moral culpability, but because the risk that the evidence would have been detrimental rather than favorable should fall on the party responsible for its loss.").

lost evidence and the amount of prejudice the requesting party has suffered because of the loss.[231]

These differing approaches to the required level of culpability for sanctions are also evident in the amendments to Rule 37. When first proposed, the Advisory Committee offered two versions; one version was in the text of the proposed rule while the other version was in a footnote.[232] The text version adopted a negligence approach and required "the party seeking protection under the proposed rule [to] have taken *reasonable steps* to preserve information after it knew the information was discoverable in the action."[233] The footnote version contained a higher culpability threshold in which sanctions would not be imposed unless the party had acted intentionally or recklessly in failing to preserve the information.[234] After extensive public comment on the two approaches, the Advisory Committee revised Rule 37(f) to adopt an intermediate culpability standard.[235]

B. Determining Relevance of Destroyed Digital Data and the Resulting Prejudice from its Destruction

When faced with a request for sanctions for the destruction of evidence, in addition to addressing the culpability of the party responsible for the loss, courts also consider whether "the destroyed evidence was 'relevant' to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense."[236] Within this context, the relevance standard goes beyond the confines of Rule 401 of the Federal Rules of Evidence.[237] The requesting party must show that the destroyed evidence "'would have been of the nature alleged by the party affected by its destruction.'"[238] Thus, to show that the destroyed evidence was "relevant," there must be some corroboration of the requesting party's claim that the destroyed evidence would have been unfavorable to the destroying party or

231. *See, e.g.*, Zubulake v. UBS Warburg, LLC (*Zubulake V*), 229 F.R.D. 422, 431 (S.D.N.Y. 2004) (citing *Residential Funding*, 306 F.3d at 108–19) (noting that the relevance of the destroyed evidence will encompass both the ordinary meaning of relevance and inference that the evidence would have been favorable to the party seeking it); *Trigon*, 204 F.R.D. at 286 (noting the "[t]he natural consequence of spoliation is that the moving party was prejudiced by the destruction"); *Turner*, 142 F.R.D. at 76–77 (discussing the necessary nexus between the suggested inference and the actual content of the destroyed evidence).

232. JUDICIAL CONFERENCE REPORT, *supra* note 19, app. C, at 84.

233. *Id.* (emphasis added).

234. *Id.*

235. *Id.* app. C, at 84–85; *see infra* Part III.C.

236. Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 220 (S.D.N.Y. 2003) (citing Byrnie v. Town of Cromwell, Bd. of Educ., 243 F.3d 93, 107–12 (2d Cir. 2001)) (adding that when evidence is destroyed in bad faith, the relevance of the evidence will be presumed).

237. FED. R. EVID. 401 ("'Relevant evidence' means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.").

238. Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108–09 (2d Cir. 2002) (quoting Kronisch v. United States, 150 F.3d 112, 127 (2d Cir. 1998)).

favorable to the requesting party.[239] This corroboration requirement, while difficult to meet, is not insurmountable. When a corporate defendant allowed all its technical e-mails to be deleted under a document retention policy, the court found that the plaintiff had met its burden to show relevance and resulting prejudice to its case because the plaintiff submitted an affidavit of one of the defendant's former employees, which described the "extensive use of e-mail" at the defendant's plants.[240]

In other cases, however, this burden has not been met. In *Drnek v. Variable Annuity Life Insurance*,[241] a securities fraud litigation, the court refused to award sanctions when the defendant implemented a new e-mail document retention policy after the claim was filed, possibly deleting potentially relevant e-mails.[242] Because the plaintiff had no specific evidence that the policy was intended to destroy relevant e-mails or actually did so, sanctions were denied.[243]

Many courts requiring bad faith have also required a separate showing of prejudice.[244] Thus, in cases dependent on electronic evidence, the requesting party has two significant hurdles to overcome: that the destroyed evidence would have been relevant and that the destruction will prejudice the party's case. Litigants can show prejudice when, as a result of digital destruction, their ability to obtain consulting and expert advice is compromised, or they are left with hard to find witnesses with fading memories and a lack of other documentary evidence that has long since been destroyed.[245]

C. A New Safe Harbor Under Proposed Rule 37(f)

The safe harbor under proposed Rule 37(f) is meant to address the appropriateness of sanctions when the loss of digital information is a result of the

---

239. *Zubulake IV*, 220 F.R.D. at 221 (citing *Residential Funding*, 306 F.3d at 108–09).

240. Mosaid Techs. Inc. v. Samsung Elecs. Co., 348 F. Supp. 2d 332, 336 (D.N.J. 2004); *see also* DaimlerChrysler Motors v. Bill Davis Racing, Inc., No. Civ.A. 03-72265, 2005 WL 3502172, at *2 (E.D. Mich. Dec. 22, 2005) (granting an adverse inference instruction for the destruction of internal e-mails when testimony confirmed that the defendant used e-mail communication extensively in its operations).

241. No. CIV 01-242-TUC-WDB, 2004 WL 1098919 (D. Ariz. May 4, 2004).

242. *Id.* at *3.

243. *Id.* Similarly, in a case involving a savings and loan claim, underwriting files were destroyed contrary to the defendant's own document retention policy after the defendant already had notice of the claim, and a document request had been made before the destruction. *See* Fed. Sav. & Loan Ins. Corp. v. Transamerica Ins. Co., 705 F. Supp. 1328, 1333 (N.D. Ill. 1989). The plaintiff tried to argue that the defendant's conduct should preclude an award of summary judgment in the defendant's favor, but because the plaintiff failed to explain how the contents of the home office file were relevant to its arguments against the defendant, the court granted summary judgment for the defendant on that claim. *Id.* at 1339 n.5.

244. *See, e.g.*, Concord Boat Corp. v. Brunswick Corp., No LR-C-95-781, 1997 WL 33352759, at *8 (E.D. Ark. Aug. 29, 1997), *rev'd on other grounds*, 207 F.3d 1039 (8th Cir. 2000) (finding that "even if the deleted e-mails were relevant to Plaintiffs' case, Plaintiffs have not suffered the requisite prejudice necessary for the giving of an adverse inference instruction").

245. *See* Trigon Ins. Co. v. United States, 204 F.R.D. 277, 290–91 (E.D. Va. 2001); William T. Thompson Co. v. Gen. Nutrition Corp., 593 F. Supp. 1443, 1450–51 (C.D. Cal. 1984).

routine operation of the party's electronic information system.[246] Proposed Rule 37(f) states: "Electronically stored information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."[247] The safe harbor would only apply to sanctions under the rules and "appears designed to accommodate the destructive tendencies of machines, rather than their human masters."[248] Certain deletions of electronic information are automatic, as when backup tapes are recycled or deleted information is overwritten.[249] Yet the lack of accountability for these "automatic" deletions is troubling. Certainly a human decision is made concerning the scheduling of automatic deletions, particularly with respect to backup tapes and archival information.

In defining "good faith" under the proposed rule, the committee notes offer the following guidance concerning the potential conflict between the destruction of electronically stored information under a routine electronic information system and the preservation obligation:

> Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation. A preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case. The good faith requirement of Rule 37(f) means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. . . . Among the factors that bear on a party's good faith in the routine operation of an information system are the steps the party took to comply with a court order in the case or party agreement requiring preservation of specific electronically stored information.[250]

---

246. JUDICIAL CONFERENCE REPORT, *supra* note 19, app. C, at 86.

247. *Id.*

248. Carol E. Heckman, *A Safe Harbor*, N.Y.L.J. Nov. 30, 2004, at 5 (stating further that "[e]-mails were obviously at the forefront of the committee's concerns in formulating the proposed amendment. . . . But the protection only applies to (1) cases where there is no court order requiring preservation of documents, and (2) loss of information that occurs after, not before, an action is commenced. These limitations, along with the lack of a bad faith standard, have lead commentators to critique the proposal as too narrow in scope to address the extent of the problem").

249. "The 'routine operation' of computer systems includes the alteration and overwriting of information, often without the operator's specific direction or awareness, a feature with no direct counterpart in hard-copy documents. Such [automatic] features are essential to the operation of electronic information systems." JUDICIAL CONFERENCE REPORT, *supra* note 19, app. C, at 87.

250. *Id.*

Absent any party or case agreement concerning preservation, a party using an electronic information system must make its own determination as to the scope and timing of any preservation efforts, and hope that those efforts satisfy the good faith standard.

The conflict between the good faith standard in Rule 37(f) and the discoverability of information on sources that are not reasonably accessible under Rule 26(b)(2) also creates tension between the two rules.[251] The committee notes advise:

> Whether good faith would call for steps to prevent the loss of information on sources that the party believes are not reasonably accessible under Rule 26(b)(2) depends on the circumstances of each case. One factor is whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources.[252]

In addition to the uncertainty created by the use of a case-by-case analysis under these circumstances, the only guidance provided in the committee notes fails to address the realities of the discovery process. The point in time at which a party would know what information was *not* available from reasonably accessible sources would be at the *end* of the discovery stage. In many cases, the operation of the electronic information system to relegate, and later destroy, potentially relevant information to an inaccessible source would occur well before the end of the discovery stage of a dispute. It would seem highly unlikely that a court would expect a party to have such a level of clairvoyance in order to determine good faith.[253] Even if there is a duty to preserve evidence, as one recent case has shown, that preservation obligation does not include "a duty to keep the data in an accessible format."[254]

---

251. The court can limit discovery generally if "the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues." FED. R. CIV. P. 26(b)(2)(iii).

252. JUDICIAL CONFERENCE REPORT, *supra* note 19, app. C, at 87. The reminder concerning the preservation obligation seems to carry little weight when combined with permissible excuses for the destruction of electronically stored information.

253. *See* Ramasastry, *supra* note 134 ("Without clearer rules, a 'reasonableness' standard may end up punishing the innocent—companies whose good faith e-preservation methods weren't up-to-the [ ] minute. It may also end up letting the guilty free—if companies' quick deletion systems are deemed acceptable (because common), even though they leave plaintiffs with scant discovery to review.").

254. Quinby v. WestLB AG, No. 04Civ.7406(WHP)(HBP), 2005 WL 3453908, at *8 n.10 (S.D.N.Y. Dec. 15, 2005). In this employment discrimination case, the plaintiff sought e-mail evidence, which the defendant claimed in an affidavit was only available on backups and would be very expensive to restore. At a later deposition of the defendant's chief information officer, the plaintiff learned that alternative, yet incomplete, sources were available to retrieve some of the e-mails. *Id.* at *2–3. The plaintiff also learned that even after the defendant became aware of her claim, the defendant converted certain potentially relevant archives from an accessible to an inaccessible format. *Id.* at *8 n.10. Despite plaintiff's claim that the defendant's actions had frustrated the discovery process, the court refused to

Moreover, without guidance as to what constitutes a "routine" record retention system, the rules appear to encourage companies to adopt systems that quickly overwrite or delete particular types of digital information, such as e-mails. Under the proposed rules, such a policy could avoid the risk of sanctions despite the possibility of destroying potentially relevant and critical information. When electronically stored information is involved in potential litigation, the party controlling that information has little incentive to preserve it. Arguments postponing the duty to preserve digital evidence until a specific discovery request has been made have been fairly successful in some cases.[255] Moreover, case law and proposed new rules of civil procedure limit the scope of the duty to preserve by creating a two-tiered discovery system that puts inaccessible data outside the reach of traditional discovery standards. Even if a litigant can establish that there was a duty to preserve electronic evidence, case law and the proposed new safe harbor raise more obstacles to the preservation. By permitting parties to excuse destruction due to document retention policies, and by requiring stringent standards of culpability and clear showings of relevance and prejudice, the threat of sanctions becomes a paper tiger. The duty to preserve electronic evidence can only be sustained through concerted, proactive efforts.

IV. PROACTIVE STEPS TO PRESERVE THE DUTY TO PRESERVE

Litigants have many options to remind opposing parties of their duty to preserve evidence: they can send a notice of preservation,[256] use early "meet and confer" opportunities under the Federal Rules of Civil Procedure,[257] or move for an order of preservation[258] (sometimes within the context of an ex parte seizure

---

grant any sanctions. *Id.*

255. *See supra* notes 54–56 and accompanying text; *see also* Redish, *supra* note 82, at 572 (arguing that this is the proper point for the duty to attach if the producing party does not object). *But see* Rambus, Inc. v. Infineon Techs. AG, 220 F.R.D. 264, 284–87 (E.D. Va. 2004) (conducting in camera review to determine if crime/fraud exception applies when a party instituted a document retention policy when it knew that litigation was likely and the document retention policy was intended to avoid high discovery costs later on); Rambus, Inc., v. Infineon Techs. AG, 222 F.R.D. 280, 292–93, 298 (E.D. Va. 2004) (applying the crime/fraud exception).

256. *See, e.g.*, Heveafil Sdn. Bhd. v. United States, 23 I.T.R.D. (BNA) 1146, 1150 (Ct. Int'l Trade 2001) (finding that the plaintiff failed to act to the best of its ability when six months after receiving notice from the Department of Commerce about the duty to maintain its source documents, it deleted the relevant data from its computer system).

257. FED. R. CIV. P. 26(f).

258. Linnen v. A.H. Robins Co., 10 Mass. L. Rep. 189, 193 (Super. Ct. 1999) (noting that the court entered a preservation order on the same day that plaintiffs filed the complaint). The *Manual for Complex Litigation* recommends that "[b]efore discovery starts, and perhaps before the initial conference, the court should consider whether to enter an order requiring the parties to preserve and retain documents, files, data, and records that may be relevant to the litigation." MANUAL FOR COMPLEX LITIGATION (FOURTH) § 11.442 (2004). One commentator has suggested that the proposed amendments to the discovery rules will "profoundly affect" the importance of the meet and confer requirements. *See* Carolyn Southerland, *Ignorance of IT Minutiae No Excuse for Litigators*, NAT'L L.J., July 17, 2006, at S1.

order).[259] Under the proposed Federal Rules of Civil Procedure, parties will be required to discuss electronic discovery issues early in the litigation, and some existing local rules already have such requirements.[260] While all these strategies help to promote the preservation of electronic evidence, each has its own cautions and difficulties.

A. Preserving the Duty to Preserve with Pre-Litigation Notice

When litigants make an effort to apprise opposing parties of the relevance of electronic data and the opposing party's corresponding duty to preserve that evidence, courts are more likely to recognize the duty and sanction a party for a failure to meet that duty. For example, in *William T. Thompson Co. v. General Nutrition Co.*,[261] the court ordered a default judgment and sanctions exceeding $450,000 for the defendant's destruction of evidence. In this antitrust action, the court found that the parties' pre-litigation correspondence provided notice concerning the need to preserve financial data.[262] In another case, evidence of meetings and internal memoranda generated by the party responsible for the destruction sufficed to attach a duty to preserve evidence.[263]

---

259. An ex parte seizure order authorizes the seizure and impoundment of relevant evidence and can be obtained without notice to the adverse party only if ex parte orders are authorized by statute or rule. *See, e.g.*, 15 U.S.C. § 1116(d)(1)(A) (2000) (providing that a court can grant an ex parte seizure order in certain situations involving counterfeit goods); 17 U.S.C. § 503(a) (2000) (allowing a court to issue an impounding order in certain copyright infringement cases); FED. R. CIV. P. 65(b) (allowing an order to be granted without written or oral notice to the opposing party if certain conditions are met). Although ex parte orders are the most effective means to guarantee the duty to preserve electronic evidence, they are also the most difficult to obtain because of the due process issues involved when a court authorizes seizure of property without providing notice to the property owner.

In addition to posting a bond equal to the value of the seized property, the litigant must provide a sworn affidavit showing that: "(1) immediate and irreparable injury, loss, or damage will result to the applicant before the adverse party . . . can be heard in opposition, and (2) . . . the efforts, if any, which have been made to give the notice and the reasons supporting the claim that notice should not be required." FED. R. CIV. P. 65(b). Although not required, courts also consider the following issues when deciding whether an ex parte seizure order is appropriate: "(1) the movant's likelihood of success on the merits of his claim; (2) whether another less drastic and adequate remedy is available; (3) a balancing of hardships between the parties; and (4) the effect of the order on the public interest." COHEN & LENDER, *supra* note 4, § 2.03[C] (noting that this is a difficult burden to meet without discovery or some other source of knowledge of the opponent's computer system and document retention policy); *see* 13 JAMES WM. MOORE ET AL., MOORE'S FEDERAL PRACTICE ¶ 65.36 (3d ed. 1997).

260. *See* JUDICIAL CONFERENCE REPORT, *supra* note 19, app. C, at 26–27; *see, e.g.*, D.N.J. CIV. R. 26.1(d) (specifying special discovery duties related to digital information).

261. 593 F. Supp. 1443, 1456 (C.D. Cal. 1984).

262. *Id.* at 1446. The court noted that the defendant was clearly on notice based on the pre-litigation correspondence: the complaint filed in August 1978, the requests for discovery served in August and September 1978, a stay order entered in October 1978, and a preservation order in July 1979. *Id.* at 1446–47. Despite all these attempts at notice, neither the company nor its counsel instructed the defendant's employees of their duty to preserve evidence. *Id.* at 1447.

263. *See* Capellupo v. FMC Corp., 126 F.R.D. 545, 546–47, 550 (D. Minn. 1989) (finding that pre-litigation contacts provided notice of the defendant's duty to preserve evidence). For examples of pre-litigation preservation letters, see SHARON D. NELSON ET AL., THE ELECTRONIC EVIDENCE AND

Attempts to remind an opposing party of its preservation obligation may fail, however, if the notice is too broad. In a class action sexual harassment claim, the plaintiff requested that the defendant preserve all electronic materials and records relevant to the lawsuit in a letter sent two days after the complaint was filed.[264] Despite the plaintiff's detailed descriptions of electronic data and her request to communicate the contents of the letter to the defendant's employees, the defendant continued its normal document retention and destruction policies and destroyed potentially relevant backup tapes and former employees' hard drives, including the hard drive of the plaintiff's former supervisor.[265] Despite this careful attempt to remind the opposing party of what electronic evidence should be preserved, the opposing party continued on with its routine document retention policy without making any attempt to search for relevant information before everything was destroyed.[266] Regardless of whether the court imposed sanctions against the defendant, the defendant's actions breached the primary goal of preserving electronic evidence.

Informal notice, as demonstrated in *Wiginton*, is fraught with peril. If the notice is too specific, the opposing party may use that pre-litigation notice as permission to destroy everything else. If the notice is too broad, the opposing party may simply ignore it. Unilateral attempts to preserve the duty to preserve are simply ineffective because they provide no opportunity for a "meeting of the minds" between the parties. While recent case law has emphasized the role of counsel to monitor a party's compliance with the duty to preserve,[267] the contours of this duty to monitor compliance may require something more than mere unilateral reminders.

B. Preservation Efforts Under the Federal Rules of Civil Procedure

The first opportunity for opposing parties to review electronic discovery issues under the current Federal Rules of Civil Procedure does not arise until the Rule

---

DISCOVERY HANDBOOK 71–89 (2006).

264. Wiginton v. CB Richard Ellis, Inc. (*Wiginton I*), No. 02 C 6832, 2003 WL 22439865, at *1 (N.D. Ill. Oct. 27, 2003). The letter specifically described electronic data and storage media including: "1) type of files; 2) on-line data storage; 3) off-line data storage; 4) data storage devices that were replaced; 5) fixed drives on personal computers and workstations; 6) programs and utilities; 7) system modification logs; 8) personal computers; and 9) evidence created subsequent to the letter." *Id.* The plaintiff further instructed the defendant:

> [T]o preserve all e-mails, both sent and received, whether internally or externally; all word-processed files, including drafts and revisions; all spreadsheets, including drafts and revisions; all databases; all presentation data or slide shows produced by presentation software . . . all Internet and Web-browser-generated history files, caches and "cookies" files generated at the work station of each employee and/or agent in [the defendant's] employ and on any and all backup storage media.

Id.; *see also* Treppel v. Biovail Corp., 233 F.R.D. 363, 368, 372 (S.D.N.Y. 2006) (finding that the plaintiff's letter to defendant describing protocols for electronic data preservation and subsequent request for a preservation order was premature).

265. *Wiginton I*, 2003 WL 22439865, at *2.

266. *Id.* at *7.

267. *See supra* notes 163–81 and accompanying text.

26(f) conference,[268] which is held at least twenty-one days before the scheduling conference required under Rule 16(b).[269] Orders pursuant to Rule 16(b) are due within 120 days after service of the complaint on the defendant.[270] Thus, digital preservation issues may not come to light until approximately three months after the filing of the complaint. Considering the recycling schedules of many document retention policies, relevant electronic evidence can be long gone by then. Although some suggest that a duty to preserve electronic evidence should not attach until a formal discovery request,[271] the standard process under the current Federal Rules of Civil Procedure fails to enhance the preservation of electronic evidence.

Parties can, of course, move for expedited discovery under Rule 26(d) before the Rule 26 initial disclosures or even before the Rule 26(f) conference.[272] In *Advantacare Health Partners, LP v. Access IV*,[273] the plaintiffs sought expedited discovery and a temporary restraining order (TRO) when a former employee appeared to have taken client lists, practice forms, and other information for use at a new, competing business.[274] The plaintiffs attempted to safeguard data with a TRO that prohibited the defendants from copying, using, or destroying any of the plaintiffs' account records, policies, or procedures.[275] Although the TRO and Notice of Expedited Discovery were served on the defendant at 4:20 p.m. on October 6, 2003, by 9:00 p.m. that evening, the defendant had installed a file deletion program and had deleted more than 13,000 files from his home computer, as well as files from his office computer and server.[276] Along with the risk that expedited discovery may not prevent the destruction of evidence, a request for expedited discovery also requires that a party already have a fairly detailed understanding of the opposing party's computing infrastructure:

> To obtain expedited discovery of electronic evidence, the movant must show that he has reasonable grounds to believe that the

---

268. FED. R. CIV. P. 26(f). Under the proposed changes to the federal discovery rules, Rule 26(f) would be amended to require that the parties address electronic discovery issues. Under proposed Rule 26(f), parties must "discuss any issues relating to preserving discoverable information, . . ." and the Discovery Plan described in proposed Rule 26(f)(3) includes "(3) any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced." JUDICIAL CONFERENCE REPORT, *supra* note 19, app. C, at 31–32.

269. FED. R. CIV. P. 26(f). The proposed amendments to Rule 16(b) would include electronic discovery issues in the content of the scheduling order. JUDICIAL CONFERENCE REPORT, *supra* note 19, app. C, at 26. Permitted contents would provide "for disclosure or discovery of electronically stored information" and adopt the parties' agreement for protection against waiving privilege. *Id.* app. C, at 26–27.

270. FED. R. CIV. P. 16(b).

271. *See supra* notes 54–56 and accompanying text.

272. FED. R. CIV. P. 26(d).

273. No. C 03-04496 JF, 2004 U.S. Dist. LEXIS 16835 (N.D. Cal. Aug. 17, 2004).

274. *Id.* at *3–5.

275. *Id.* at *4.

276. *Id.* at *5–6. Despite the defendant's actions, which the court deemed as clearly in bad faith and prejudicial, the court refused to award the most severe sanction of a default judgment and instead allowed an adverse inference instruction and a fine of $20,000. *Id.* at *16–17, *20–21, *31.

> opposing party is destroying relevant electronic evidence and that this destruction will cause irreparable harm to the moving party. Moreover, a party should be prepared to provide sufficient information concerning the opposing party's computer system and information retention practices in order to establish both elements required for a successful motion to expedite the discovery process. The movant should also narrowly tailor his request to the greatest extent possible and explicitly reserve the right to conduct further discovery in the ordinary course of the litigation.[277]

In addition to a request for expedited discovery, a related strategy involves a request for limited discovery, prior to Rule 26(a)(1) initial disclosures, concerning the opposing party's computing infrastructure. Under Rule 30(b)(6), a litigant can request limited discovery and depose the computer personnel who have knowledge of the party's data networks and storage systems.[278] Instead of depositions, one court has suggested that interrogatories under Rule 33 are more efficient discovery vehicles for determining the contours of an organization's information infrastructure.[279] In any litigation involving a commercial entity, the court and parties need to consider issues concerning the preservation of electronic evidence. While using the expedited discovery process is sometimes inappropriate, courts and parties should not ignore the critical need to take affirmative steps to preserve electronic evidence. In some cases, litigants may need to take more proactive steps, such as requesting a preservation order from the court.

C. Preserving the Duty to Preserve by Moving for a Preservation Order

The cases of digital destruction that have garnered the most attention because of the severe sanctions imposed have something in common: the opposing litigants made the preservation duty crystal clear through the use of court imposed preservation orders.[280] Although these cases suggest that preservation orders are needed to remind litigants of their duty to preserve relevant electronic evidence,

---

277. COHEN & LENDER, *supra* note 4, § 2.05; *see also* Physicians Interactive v. Lathian Sys., Inc., 69 U.S.P.Q.2d (BNA) 1981, 1984–85, 1989 (E.D. Va. Dec. 5, 2003) (finding that the plaintiff in a civil action against alleged computer hackers met the tests for a preliminary injunction and expedited discovery, thus allowing the plaintiff to enter the site where the defendant's computers were located and make "mirror" or bitstream images of the hard drives, provided that the imaging be done by a computer forensics expert and that discovery be limited to information related to the alleged attacks).

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

279. *See* Treppel v. Biovail Corp., 233 F.R.D. 363, 373–74 (S.D.N.Y. 2006) (condoning the plaintiff's use of a "Document Retention Questionnaire" and treating the questionnaire as an acceptable interrogatory).

280. *See, e.g.*, United States v. Philip Morris USA, Inc., 327 F. Supp. 2d 21, 23, 26 (D.D.C. 2004) (ordering a sanction of $2.75 million when the defendant destroyed e-mails after a preservation order had made clear the duty to preserve the e-mails); *In re* Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598, 600, 616–17 (D.N.J. 1997) (granting sanctions of a $1 million fine and attorney fees for document destruction after a preservation order was in place).

some courts have found that because of the common law and applicable statutory duties to preserve evidence, preservation orders are not really needed and courts should only grant them upon the more stringent standard for preliminary injunctions.[281] In addition, committee notes to the proposed amendments of the discovery rules also seem to echo a restrictive view on the use of preservation orders. The proposed committee note to Rule 26(f) states: "The requirement that the parties discuss preservation does not imply that courts should routinely enter preservation orders. A preservation order entered over objections should be narrowly tailored. Ex parte preservation orders should issue only in exceptional circumstances."[282] Thus, attempts to preserve the duty to preserve may face an additional hurdle.

A preservation order requires a party to preserve electronic evidence even if compliance means the party must disable or suspend routine document retention and destruction policies. A court can base authority for a preservation order on its inherent powers concerning case management and on Federal Rule of Civil Procedure 16(c), which provides that a court may take appropriate action with respect to "the control and scheduling of discovery, including orders affecting disclosures and discovery[,] . . . the need for adopting special procedures for managing potentially difficult or protracted actions that may involve complex issues . . . or unusual proof problems . . . [and any] matters as may facilitate the just, speedy, and inexpensive disposition of the action."[283] Despite the authority in the federal rules, litigants face significant legal, as well as practical, challenges when attempting to obtain a protective order.

Litigants may argue that in light of the common law duty to preserve evidence, as well as an attorney's ethical duties, preservation orders are unnecessary. As one court stated:

> Whenever a lawsuit is filed, the defendant is automatically required to take all appropriate steps to preserve any and all information which might be relevant to that litigation. To supplement every complaint with an order requiring compliance with the Rules of Civil Procedure would be a superfluous and

281. *See* Pepsi-Cola Bottling Co. v. Cargill, Inc., Civ. No. 3-95-784, 1995 WL 783610, at *3–4 (D. Minn. Oct. 20, 1995) (citing *In re* Potash Antitrust Litig., No. 3-93-197, MDL No. 981, 1994 WL 1108312, at *8–9 (D. Minn. Dec. 5, 1994)).

282. JUDICIAL CONFERENCE REPORT, *supra* note 19, app. C, at 35. In addition, all references to preservation orders were removed from the text of Rule 37(f) after many argued that the provision might "promote applications for preservation orders as a way to defeat application of the proposed rule." *Id.* app. C, at 84.

283. FED. R. CIV. P. 16(c)(6), (12), (16). The order should "clearly describe the scope of evidence that must be preserved, thus reducing the potential for dispute as to the sometimes unclear scope of this duty, especially with respect to electronic evidence." COHEN & LENDER, *supra* note 4, § 2.03[B]; *see also* JAMES WM. MOORE ET AL., MOORE'S FEDERAL PRACTICE ¶ 37A.11[3][b] (3d ed. 2006) (discussing the importance of a court's clear preservation order giving notice of sanctions for destroying relevant evidence).

> wasteful task, and would likely create no more incentive upon the parties than already exists.[284]

The series of events in the *Linnen* case illustrate the problems with this approach.[285] In *Linnen*, the court entered a preservation order on the same day the complaint was filed.[286] The order stated: "All defendants must take all necessary steps to assure that their employees, agents, accountants and attorneys refrain from discarding, destroying, erasing, purging or deleting any such documents including, but not limited to, computer memory, computer disks, data compilations, e-mail messages sent and received and all back-up computer files . . . ."[287] Upon the defendants' motion, the preservation order was vacated two weeks later because the court accepted the defendants' arguments that the preservation order was unduly burdensome.[288] Once the court vacated the preservation order, the plaintiff requested that the defendants sign a stipulation regarding information to be preserved during the litigation.[289] The defendants refused, stating: "We do not believe that a stipulation regarding preservation of documents is necessary. . . . [T]he defendants recognize their obligation to take reasonable steps to preserve documents relevant to the subject matter of this action."[290] Despite the defendants' assurances, the defendants continued to recycle backup tapes and were subsequently sanctioned.[291]

A litigant may face a heavy burden of proof to obtain a preservation order even when a court is willing to consider the order. One suggested balancing test to determine whether to issue a preservation order is based on the following three factors:

> (1) the level of concern the court has for the continuing existence and maintenance of the integrity of the evidence in question in the absence of an order directing preservation of the evidence; (2) any irreparable harm likely to result to the party seeking the preservation order of evidence absent an order directing preservation; and (3) the capability of an individual, entity, or party to maintain the evidence sought to be preserved, not only as to the evidence's original form, condition or contents, but also the

284. Hester v. Bayer Corp., 206 F.R.D. 683, 685 (M.D. Ala. 2001) (citation omitted). The district court vacated a state court preservation order after the complaint was removed to the federal court. *Id.* at 686. *See also Treppel*, 233 F.R.D. at 368 (describing the responding party's claim that a proposed preservation order would be "unnecessarily onerous" and that it was already well aware of its preservation obligations).

285. *See* Linnen v. A.H. Robins Co., 10 Mass. L. Rep. 189, 189–91 (Super. Ct. 1999).

286. *Id.* at 193.

287. *Id.*

288. *Id.* at 194.

289. *Id.*

290. *Id.*

291. *Id.* at 194–95.

> physical, spatial and financial burdens created by ordering evidence preservation.[292]

In addition, the litigant seeking the preservation order must show that the order is "necessary and not unduly burdensome."[293] The *Manual for Complex Litigation* explains that the court should determine if the preservation order "is needed, the scope, duration, method of data preservation, and other terms that will best preserve relevant matter without imposing undue burdens."[294] Blanket preservation orders can seriously disrupt a commercial entity's day-to-day operations and may impose preservation requirements that make no sense given the company's computing infrastructure and policies.[295] While a preservation order can help avoid the "satellite litigation" that proliferates when preservation obligations are unclear, preservation orders are not a one size fits all proposition.[296] As the court stated in *Hester v. Bayer Corp.*, "Indeed, like snowflakes, no two litigations are alike, so a

---

292. Capricorn Power Co. v. Siemens Westinghouse Power Corp., 220 F.R.D. 429, 433–34 (W.D. Pa. 2004).

293. Pueblo of Laguna v. United States, 60 Fed. Cl. 133, 138 (Fed. Cl. 2004) (citing Walker v. Cash Flow Consultants, 200 F.R.D. 613, 617 (N.D. Ill. 2001); Adobe Sys., Inc. v. S. Sun Prod. Inc., 187 F.R.D. 636, 641 (S.D. Cal. 1999)).

294. MANUAL FOR COMPLEX LITIGATION, *supra* note 259, § 11.442.

295. The *Manual for Complex Litigation* suggests that courts should consider the following points in crafting an effective preservation order:

- Continued operation of computers and computer networks in the routine course of business may alter or destroy existing data, but a data preservation order prohibiting operation of the computers absolutely would effectively shut down the responding party's business operations. Such an order requires the parties to define the scope of contemplated discovery as narrowly as possible, identify the particular computers or network servers affected, and agree on a method for data preservation, such as creating an image of the hard drive or duplicating particular data on removable media, thereby minimizing cost and intrusiveness and the downtime of the computers involved.
- Routine system backups for disaster recovery purposes may incidentally preserve data subject to discovery, but recovery of relevant data from nonarchival backups is costly and inefficient, and a data-preservation order that requires the accumulation of such backups beyond their usual short retention period may needlessly increase the scope and cost of discovery. An order for the preservation of backup data obliges the parties to define the scope of contemplated discovery narrowly to minimize the number of backups that need to be retained and eventually restored for discovery purposes.
- A preservation order may be difficult to implement perfectly and may cause hardship when the records are stored in data-processing systems that automatically control the period of retention. Revision of existing computer programs to provide for longer retention, even if possible, may be prohibitively expensive. Consider alternatives, such as having parties duplicate relevant data on removable media or retaining periodic backups.

Id. § 11.442.

296. Hester v. Bayer Corp., 206 F.R.D. 683, 685–86 (M.D. Ala. 2001).

preservation order tailored to the particular issues of the lawsuit in question may best ensure a forthright and expeditious discovery process."[297]

Given the significant economic ramifications that can ensue from a preservation order, several courts view a request for a preservation order as a request for injunctive relief and use the heightened standard of requiring the party to show irreparable harm.[298] However, in light of the increased emphasis on a judge's case management powers found in both the Federal Rules of Civil Procedure and case law, one recent decision found that:

> [A] document preservation order is no more an injunction than an order requiring a party to identify witnesses or to produce documents in discovery. . . . [T]he court sees no reason for it to consider whether plaintiff is likely to be successful on the merits of its case in deciding whether to protect records from destruction. In the court's view, such an approach would be decidedly to put the cart before the horse.[299]

As a result, the court placed more emphasis on evaluating the basis of the plaintiff's perceived threat that it needed a preservation order to prevent the destruction of evidence.[300] Although the plaintiff had requested a broad preservation order, the court considered the practical concerns raised by the defendant and granted a preservation order that included the protocols suggested by the defendant.[301] When

---

297. *Id.* at 685.

298. *See, e.g.*, Pepsi-Cola Bottling Co. v. Cargill, Inc., Civ. No. 3-95-784, 1995 WL 783610, at *3 (D. Minn. Oct. 20, 1995) (citing *In re* Potash Antitrust Litig., No. 3-93-197, 1994 WL 1108312, at *8 (D. Minn. Dec. 5, 1994) (noting that in both the instant case and *Potash*, the plaintiffs did not show that the court's denial of the order would cause irreparable harm); *In re Potash*, 1994 WL 1108312, at *8 (finding the defendant's argument persuasive that issuing a preservation order is an exercise of injunctive powers). Although the test for injunctive relief may vary among the circuits, generally courts require a party seeking injunctive relief to establish the following: (1) a likelihood of ultimate success on the merits of the moving party's claim, (2) irreparable harm to the moving party if the injunction is not granted, (3) proof that the threatened injury outweighs the harm to the party to be enjoined, and (4) a showing that the public interest favors the moving party. *See, e.g.*, KOS Pharms., Inc. v. Andrx Corp., 369 F.3d 700, 708 (3d Cir. 2004) (citing Allegheny Energy, Inc. v. DQE, Inc., 171 F.3d 153, 158 (3d Cir. 1999)) (stating the four factors); Dominion Video Satellite, Inc. v. Echostar Satellite Corp., 356 F.3d 1256, 1260 (10th Cir. 2004) (citing Prairie Band of Potawatomi Indians v. Pierce, 253 F.3d 1234, 1246 (10th Cir. 2001)) (stating the four factors); *In re* Microsoft Corp. Antitrust Litig., 333 F.3d 517, 526 (4th Cir. 2003) (citing Safety-Kleen, Inc. v. Wyche, 274 F.3d 846, 858–59 (4th Cir. 2001)) (stating the four factors); Overstreet v. Lexington-Fayette Urban County Gov't, 305 F.3d 566, 573 (6th Cir. 2002) (citing Leary v. Daeschner, 228 F.3d 729, 736 (6th Cir. 2000)) (stating the four factors).

299. Pueblo of Laguna v. United States, 60 Fed. Cl. 133, 138 n.8 (Fed. Cl. 2004) (citations omitted) (finding that "courts need not observe the rigors of the four-factor analysis ordinarily employed in issuing injunctions"); *accord* Treppel v. Biovail Corp., 233 F.R.D. 363, 370–72 (S.D.N.Y. 2006) (applying a balancing test and denying a request for a preservation order as "premature").

300. *See Pueblo of Laguna*, 60 Fed. Cl. at 138. The plaintiff submitted information concerning a related litigation with the Department of the Interior in which document destruction had been rampant. *Id.*

301. *Id.* at 140–41.

a preservation order is crafted to meet the special needs of the litigation, it can be a powerful tool to preserve the duty to preserve.

V. CONCLUSION

Although we are not yet a paperless society, we are fast approaching a landscape where a large proportion of an organization's information is digital. Many legal disputes in litigation areas such as employment discrimination, product liability, securities fraud, and the infringement of intellectual property involve business entities. As these litigants seek to meet their burden of proof, the facts will exist in an increasingly fragile state. The extent to which that information is accessible is entirely in the hands of its keepers. As developing case law and the Federal Rules of Civil Procedure combine to send the message that organizations should not be burdened with the need to preserve or retrieve inaccessible electronic data, electronically stored information will find itself subject to retention policies that ensure an organizational "Alzheimer's."

Although the need of a business entity to manage its digital information in an efficient manner is certainly important, the need to maintain an institutional memory lies at the core of our judicial system. As one court stated:

> Th[e] duty of disclosure would be a dead letter if a party could avoid the duty by the simple expedient of failing to preserve documents that it does not wish to produce. . . .
>
> Parties and attorneys frequently are called upon to preserve and produce documents that are against their interest. . . . [W]hen they do so, the parties and the attorneys uphold the integrity of our litigation system and inspire confidence in it.[302]

Therefore, in recognition of the fragile nature of electronic information, affirmative steps are needed. Technology in data storage and retrieval continues to evolve and improve. With the continuing improvement of data storage capabilities, courts should evaluate an organization's information retention policy on the basis of the organization's good faith effort to manage its information in a responsible manner. Electronic information, especially e-mail communication, covering employment matters and product development, for example, should not be subject to unreasonably short retention periods.

Litigants and their attorneys must be proactive in handling issues related to electronic discovery. Being proactive does not mean cluttering the courts with automatic filings for preservation orders; it does mean, however, using the existing procedural framework to understand the capabilities and the limits of an opposing party's computing infrastructure and policies. In this sense, the proposed amendments to the federal discovery rules that encourage the early recognition of potential issues concerning electronic evidence are a step in the right direction. In

302. Danis v. USN Commc'ns, Inc., 53 Fed. R. Serv. 3d (West) 828, 829 (N.D. Ill. 2000).

contrast, however, changes in the rules that permit litigants to place information out of reach through self-determined technological inaccessibility or unquestioned document retention policies increase the vulnerability of electronic evidence. The integrity of our legal system demands that courts and litigants understand their role in preserving the duty to preserve.