

*Chapter 2*

# Preservation of Electronically Stored Information

Todd L. Nunn

Michael Goodfried

Ted Webber

[Return to book table of contents](#)

---

TODD L. NUNN is a partner in the Document Analysis Technology Group (“DATG”) at Preston Gates Ellis in Seattle. His practice focuses on e-discovery and complex document production, class action defense, and insurance coverage. Todd is a frequent writer and speaker on e-discovery issues, and is the Chairman of the Electronically Stored Information Discovery Subcommittee, a subcommittee of the Washington State Bar Association Court Rules and Procedures Committee that is considering e-discovery specific amendments to the Washington State Court Rules.

Co-authors MICHAEL GOODFRIED and TED WEBBER are staff attorneys in DATG at Preston Gates Ellis whose practices focus on e-discovery and complex document production. Co-author Trudy Tessaro is an attorney in the firm’s Business Litigation Group and DATG who contributes to DATG’s Blog at [www.ediscoverylaw.com](http://www.ediscoverylaw.com).

# Preservation of Electronically Stored Information

## Table of Contents

- Introduction ..... 19
- The Duty to Preserve Evidence..... 19
  - When Does the Duty to Preserve ESI Begin?..... 20
  - Scope of the Duty to Preserve ..... 21
  - When Does the Duty to Preserve End? ..... 22
  - Possible Consequences When the Duty to Preserve is Not Met ..... 22
- Unique Preservation Issues Presented by Electronic Data ..... 29
- Records Management—Document Retention and Destruction Policies..... 30
  - Companies Should Consider Implementing and Following a Document Retention Policy..... 30
  - Considerations for a Reasonable Document Retention Policy..... 30
  - Legal Hold Notices as a Best Practice of Document Retention ..... 32
  - Retention Considerations for Disaster Recovery Systems..... 33
- Legal Hold Notices..... 34
  - Scope of the Legal Hold Notice ..... 34
  - Implementing a Legal Hold Notice..... 36
  - Contents of a Legal Hold Notice..... 37
  - Implement a Policy to Preserve Documents from Employees who Leave the Company ..... 38
  - Ensuring Preservation—Collection of Documents ..... 38
- Preservation Issues for Parties Seeking Discovery of Electronic Documents..... 39
  - Address Preservation of Evidence Concerns Early ..... 39
  - Consider Notifying Opposing Counsel in Writing..... 39
  - If Circumstances Warrant, Obtain a Preservation Order from the Court..... 40
  - If Relevant Evidence Is Destroyed, Consult a Computer Forensics Expert and Consider Seeking
    - Appropriate Sanctions..... 41
  - Review Material Produced and Follow Up Promptly..... 41
  - Employ Other Discovery Tools ..... 42



# Preservation of Electronically Stored Information

## Introduction

“It goes without saying that a party can only be sanctioned for destroying evidence if it had a duty to preserve it.”<sup>1</sup> If a company has no such duty, then it cannot be faulted.<sup>2</sup>

This chapter discusses the legal issues related to the preservation of electronically stored information (“ESI”). It discusses the duty to preserve evidence—what it is, when it applies, and the consequences that may result if the duty is not met. This chapter also discusses the unique challenges presented by electronic data, and how document retention policies and legal hold notices can be used to help manage ESI—including practical tips and checklists to help litigants take reasonable and appropriate steps to preserve ESI and avoid claims of spoliation. Finally, this chapter discusses the preservation issues that face parties seeking discovery of ESI.

## The Duty to Preserve Evidence

What is the duty to preserve email and electronic documents in litigation? It may accurately be characterized as a duty to prevent spoliation of evidence.<sup>3</sup> Spoliation is “the destruction or significant alteration of evidence, or the failure to preserve property for another’s use as evidence in pending or reasonably foreseeable litigation.”<sup>4</sup> The factors that determine whether spoliation occurred vary by jurisdiction,<sup>5</sup> but generally there must be a showing that evidence has been destroyed after the

party knew, or should have known, that the material in question may be relevant to litigation.

As a general rule, a duty to preserve evidence arises once a party has notice of its relevance.<sup>6</sup> The Eighth Circuit has held 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.”<sup>7</sup> Another formulation of the duty to preserve rule states that:

While a litigant is under no duty to keep or retain every document in its possession once a complaint is filed, 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.<sup>8</sup>

There must be a specific threat or dispute to which the evidence relates. A company is not required to retain all email communications that might be relevant to some nonspecific future litigation. For example, the plaintiffs in *Concord Boat Corp. v. Brunswick Corp.*<sup>9</sup> argued that because the defendant was embroiled in various antitrust matters from 1992 to present, the defendant was under a duty to preserve all email relevant to antitrust issues from that date on. The court rejected such a broad duty, noting both the prevalence of email usage and the ever-present threat of litigation faced by large corporations.<sup>10</sup>

<sup>1</sup> *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (“Zubulake IV”).

<sup>2</sup> *Id.*

<sup>3</sup> *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583 (4th Cir. 2001).

<sup>4</sup> *Zubulake IV*, 220 F.R.D. at 216 (citing *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999)).

<sup>5</sup> *Cf. Zubulake IV*, 220 F.R.D. at 212; *Vela v. Wagner & Brown, Ltd.*, 2006 WL 1004476 (Tex. App. Apr. 19, 2006); *Durst v. FedEx Express*, 2006 WL 1541027 (D.N.J. June 2, 2006).

<sup>6</sup> *Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D. 68, 72–73 (S.D.N.Y. 1991).

<sup>7</sup> *Lewy v. Remington Arms Co., Inc.*, 836 F.2d 1104, 1112 (8th Cir. 1988).

<sup>8</sup> *Turner*, 142 F.R.D. at 72 (quoting *Wm. T. Thompson Co. v. Gen. Nutrition Corp., Inc.*, 593 F. Supp. 1443, 1455 (C.D. Cal. 1984)).

<sup>9</sup> 1997 WL 33352759 (E.D. Ark. Aug. 29, 1997).

<sup>10</sup> *Id.*, at \*4 (“to 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.... Such a proposition is not justified.”).

Identifying the particular boundaries of a litigant's duty to preserve involves two related inquiries: *when* does the duty to preserve attach, and *what* evidence must be preserved?<sup>11</sup>

### *When Does the Duty to Preserve ESI Begin?*

The duty to preserve ESI is triggered when a party has notice that the evidence is relevant to litigation, or when a party should have known that the evidence may be relevant to future litigation.<sup>12</sup>

The duty to preserve material evidence arises not only during litigation, but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation.<sup>13</sup> Determining when a party anticipates litigation requires a fact intensive inquiry, however, and a precise definition of when such anticipation occurs is "elusive."<sup>14</sup> The duty to preserve is generally triggered when litigation is "probable," "likely," or "reasonably anticipated."<sup>15</sup> Courts state the test in a number of different ways, but invariably include elements of probability and reasonableness. "The majority of courts have held that pre-litigation destruction can constitute spoliation when litigation was 'reasonably foreseeable' but not where it was 'merely possible.'"<sup>16</sup> The duty to preserve evidence does not arise "if there was merely a potential for litigation."<sup>17</sup> Thus, the fact that one or

two employees contemplate the possibility that a fellow employee might sue does not generally impose a firm-wide duty to preserve. The *Zubulake* court found that the duty was triggered when "almost everyone associated with *Zubulake* recognized the possibility that she might sue."<sup>18</sup>

Thus, one can conclude that a duty to preserve exists once a party has notice that litigation or a government investigation is already underway or is imminent. A party's obligation to preserve relevant evidence will generally be triggered upon service or receipt of any of the following:

- A draft complaint, whether or not actually filed
- Requests for production of documents
- A Civil Investigative Demand (or other agency equivalent)
- A third party subpoena
- A written request for preservation of specific documents relating to actual litigation
- A complaint filed with a regulatory body, such as the U.S. Equal Employment Opportunity Commission (EEOC)
- A written demand letter from a lawyer for a party that sets out the party's claim, describes the resolution desired, and clearly threatens litigation if the claim is not resolved

The most difficult determinations occur where liti-

<sup>11</sup> *Zubulake IV*, 220 F.R.D. at 216.

<sup>12</sup> *Id.*

<sup>13</sup> *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583 (4th Cir. 2001); *see also Kronisch v. U.S.*, 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, providing the party responsible for the destruction with express notice, 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."); *Bayoil, S.A. v. Polembros Shipping Ltd.*, 196 F.R.D. 479, 483 (S.D. Tex. 2000) ("Notice does not have to be of actual litigation, but can concern 'potential' litigation. Otherwise, any person could shred documents to their heart's content before suit is brought without fear of sanction.").

<sup>14</sup> *Samsung Elec. Co., Ltd. v. Rambus, Inc.*, 439 F. Supp. 2d 524, 542 (E.D. Va. 2006).

<sup>15</sup> *See, e.g., Zubulake IV*, 220 F.R.D. at 217.

<sup>16</sup> *Performance Chevrolet, Inc. v. Market Scan Info. Sys., Inc.*, 2006 WL 1042359 (D. Idaho Apr. 18, 2006); *see also 7 James W. Moore, MOORE'S FEDERAL PRACTICE* §37A.11[3][a], at 37A-27 (3d ed. 2003); American Bar Association, *CIVIL DISCOVERY STANDARDS*, Standard No. 10 (Aug. 1999) (The duty arises only when "litigation is probable or has been commenced."); *Hynix Semiconductor, Inc. v. Rambus, Inc.*, No. C-00-20905 RMW, slip op. at 7 (N.C. Cal. Jan. 31, 2005) (Judge Whyte framed the test as follows: "The question, then, is whether Rambus had commenced *or intended to commence litigation* at the time it implemented its document retention policy and began destroying documents.") (emphasis added).

<sup>17</sup> *Lekkas v. Mitsubishi Motors Corp.*, 2002 WL 31163722, at \*2 (N.D. Ill. Sept. 26, 2002).

<sup>18</sup> *Zubulake IV*, 220 F.R.D. at 217.

gation has not commenced, but is somewhere on the continuum of possibilities. Such situations can arise where a party receives notice of a dispute or a weak threat of litigation, is considering instigating an action themselves, or becomes aware of potential litigation through a third party source. As noted earlier, the duty to preserve relevant information does not attach in every instance where litigation is possible, only where it is probable. Whether litigation is “probable” is a highly factual matter requiring consideration of the particular circumstances at hand.

For purposes of assessing intentional spoliation, one court has suggested using the more widely developed standard for anticipation of litigation under the work product doctrine as an analytical tool to help determine the point at which litigation was reasonably foreseeable.<sup>19</sup> The work product doctrine limits the discoverability of documents and tangible things prepared in anticipation of litigation or for trial.<sup>20</sup> The established standard to determine whether the work product protection applies is that the document “must be prepared *because* of the prospect of litigation when the preparer faces an actual claim or a potential claim following an actual event or series of events that reasonably could result in litigation.”<sup>21</sup>

The following are some considerations that may be relevant to determining whether litigation is probable.

Litigation threatened or demand letter received:

- Does the communication accurately describe the event(s) giving rise to the demand? Is it consistent with the information known?
- Does the demand appear to be warranted under the facts known?
- Who authored the demand letter, and what is his/her role?
- To whom was the threat of litigation or demand letter directed, and what is his/her role?

- Is the threat of litigation explicit or merely inferred?
- Is the threat of litigation credible or does it appear specious?

Third party source, such as a news media report, suggests possible litigation:

- Is the source reliable, and does the information appear accurate based on the facts known?
- A report by the news media alone probably would not give rise to a duty to preserve; however, a duty may be triggered if the news report is coupled with other information indicating that litigation will probably ensue.

If the preserving party itself is considering litigation:

- What persons within the organization have information about the contemplated litigation? Do they have authority to bring suit? If not, have they informed the decision-maker(s) about the circumstances giving rise to the claim?
- Has legal counsel, whether in-house or outside counsel, been consulted to determine whether a cause of action may exist?
- Has the organization taken any concrete steps towards filing suit, or communicating with the adverse party about the potential claim?
- Has a demand letter been sent? Has a demand letter been researched and/or drafted?

### *Scope of the Duty to Preserve*

“To be sure, the duty to preserve does not require a litigant to keep every scrap of paper in its file.”<sup>22</sup> Corporations are not obligated, upon recognizing the threat of litigation, to “preserve every shred of paper, every e-mail or electronic document, and every backup tape.”<sup>23</sup> Indeed, “[s]uch a rule would cripple large corporations.”<sup>24</sup> “While a litigant is under no duty to keep or retain every document in its possession. . . it is under

<sup>19</sup> Samsung, 439 F. Supp. 2d at 542 (the court analogized this standard with regard to claims of intentional spoliation because there has to be a direct relationship between the anticipated litigation and the destruction of relevant evidence—similar to how work product requires a direct relation between the anticipated litigation and the creation of a document. The court noted that this analogy does not apply to claims of negligent spoliation).

<sup>20</sup> See FED. R. CIV. P. 26(b)(3); Hickman v. Taylor, 329 U.S. 495 (1947).

<sup>21</sup> Nat’l Union Fire Ins. Co. of Pittsburgh, Pa. v. Murray Sheet Metal Co., Inc., 967 F.2d 980, 984 (4th Cir. 1992).

<sup>22</sup> Danis v. USN Commc’ns, Inc., 2000 WL 1694325, at \*32 (N.D. Ill. Oct. 20, 2000).

<sup>23</sup> Zubulake IV, 220 F.R.D. at 217.

<sup>24</sup> *Id.*; see also Wiginton v. CB Richard Ellis, Inc., 2003 WL 22439865, at \*4 (N.D. Ill. Oct. 27, 2003) (“A party does not have to go to ‘extraordinary measures’ to preserve all potential evidence.”); THE SEDONA PRINCIPLES: BEST PRACTICES

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.”<sup>25</sup>

### The “Key Players”

The duty to preserve extends to any documents or tangible things (as defined by FED. R. CIV. P. 34(a)) made by individuals “likely to have discoverable information that the disclosing party may use to support its claims or defenses.” The duty includes documents prepared for those individuals as well, to the extent those documents can be readily identified. The duty also extends to information that is relevant to the claims or defenses of any party, or which is “relevant to the subject matter involved in the action.” Thus, the duty to preserve extends to those employees likely to have relevant information—the “key players” in the case.<sup>26</sup>

### What Must Be Retained?

A party’s duty to preserve specific types of documents does not arise unless the party controlling the documents has notice of those documents’ relevance.<sup>27</sup>

*Zubulake IV* instructs:

A party or anticipated party must retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any relevant documents created thereafter.<sup>28</sup>

“[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.”<sup>29</sup>

### *When Does the Duty to Preserve End?*

Because case law has yet to resolve the question of when the duty to preserve evidence ends, there is no clear guidance for deciding when a company no longer needs to preserve evidence. If a potential adversary does not follow up on its demand letter within a reasonable amount of time, shouldn’t the preservation obligation end? When in the sequence of a case should the preservation obligation end? At the conclusion of discovery? Trial? Appeal? Settlement? The preservation obligation must end at some reasonable point in time.

### *Possible Consequences When the Duty to Preserve is Not Met*

Failure to preserve potentially relevant ESI, once the duty to do so has been triggered, raises the specter of spoliation of evidence and sanctions. A court’s authority to sanction a party for the failure to preserve or produce relevant evidence is both inherent and statutory.<sup>30</sup> Whether proceeding under FED. R. CIV. P. 37 or under a court’s inherent powers, the analysis is essentially the same.<sup>31</sup> However, the power to enter a default judgment or to dismiss a case for noncompliance with a discovery order depends exclusively upon Rule 37.<sup>32</sup>

Spoliation sanctions are intended to serve one or more of the following purposes: (1) to ameliorate the prejudice caused to an innocent party by a discovery

---

RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION, Principle 5, (The Sedona Conference®, July 2005) (“The obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.”).

<sup>25</sup> *Wm. T. Thompson Co. v. Gen. Nutrition Corp., Inc.*, 593 F. Supp. 1443, 1455 (C.D. Cal. 1984).

<sup>26</sup> *Zubulake IV*, 220 F.R.D. at 217–18.

<sup>27</sup> *In re Old Banc One S’holders Sec. Litig.*, 2005 WL 3372783, at \*3 (N.D. Ill. Dec. 8, 2005).

<sup>28</sup> *Zubulake IV*, 220 F.R.D. at 218.

<sup>29</sup> *Id.* at 217.

<sup>30</sup> *Danis v. USN Commc’ns, Inc.*, 2000 WL 1694325, at \*30 (citing *Chambers v. NASCO, Inc.*, 501 U.S. 32, 50–51 (1991) (federal courts may sanction bad faith conduct by its inherent powers or by the FEDERAL RULES OF CIVIL PROCEDURE)).

<sup>31</sup> *Cobell v. Babbit*, 37 F. Supp. 2d 6, 18 (D.D.C. 1999); *Gates Rubber Co. v. Bando Chem. Indus., Ltd.*, 167 F.R.D. 90, 107 (D. Colo. 1996) (“any distinctions between Rule 37 and the inherent powers of the court are distinctions without differences”).

<sup>32</sup> *Societe Internationale Pour Participations Industrielles et Commerciales, S.A. v. Rogers*, 357 U.S. 197, 207 (1958).

violation; (2) to punish the party who violates his or her obligations; and/or (3) to deter others from committing like violations.<sup>33</sup> A district court considering the imposition of sanctions must show restraint,<sup>34</sup> and any sanction leveled must be proportionate to the harm caused.<sup>35</sup> A court is given broad discretion to choose the appropriate sanction for a discovery violation given the unique factual circumstances of each case.<sup>36</sup>

In general, courts will examine three factors in determining whether to impose sanctions for spoliation of evidence: (1) a breach of the duty to preserve or produce documents; (2) the level of culpability for the breach; and (3) the prejudice resulting from the breach, or, stated differently, whether the evidence would have been relevant to the moving party's case, in that a reasonable fact finder could conclude that the evidence would have been favorable to the moving party.<sup>37</sup>

The culpability threshold varies across jurisdictions. Some require bad faith, while others have concluded that mere negligence is sufficient.<sup>38</sup> The rationale for sanctioning even the negligent loss of evidence which should have been preserved is that it restores the "evidentiary balance" by shifting the cost to the party that destroyed evidence.<sup>39</sup>

A reasonable records retention plan can be relevant in a court's determination as to the culpability or blameworthiness of the party.<sup>40</sup> The *Lewy* court suggested the following inquiry when destruction of evidence occurs under a records retention policy:

[I]f the trial court is called upon to again instruct the jury regarding failure to produce evidence, the court should consider the following factors before deciding whether to give the instruction to the jury. First, the court should determine whether Remington's record retention policy is reasonable considering the facts and circumstances surrounding the relevant documents. For example, the court should determine whether a three year retention policy is reasonable given the particular document. A three year retention policy may be sufficient for documents such as appointment books or telephone messages, but inadequate for documents such as customer complaints. Second, in making this determination the court may also consider whether lawsuits concerning the complaint or related complaints have been filed, the frequency of such complaints, and the magnitude of the complaints.

Finally, the court should determine whether the document retention policy was instituted in bad faith. In cases where a document retention policy is instituted in order to limit damaging evidence available to potential plaintiffs, it may be proper to give an instruction similar to the one requested by the Lewys. Similarly, even if the court finds the policy to be reasonable given the nature of the documents subject to the policy, the court may find that under the particular circumstances certain documents should have been retained notwithstanding the policy. For example, if the corporation knew

<sup>33</sup> See generally *Nat'l Hockey League v. Metro. Hockey Club, Inc.*, 427 U.S. 639, 643 (1976) (noting dual purpose of punishment and deterrence); *Marrocco v. Gen. Motors Corp.*, 966 F.2d 220, 224 (7th Cir. 1997) (discussing compensatory purpose of directed verdict as sanction for prejudice resulting from lost documents: "sanctions can be employed for a wide array of purposes, but they cannot replace lost evidence"); *Telectron v. Overhead Door Corp.*, 116 F.R.D. 107, 135 (S.D. Fla. 1987) (discussing three purposes of sanctions: punishment, deterrence and compensation for prejudice).

<sup>34</sup> *Barnhill v. U.S.*, 11 F.3d 1360, 1368 (7th Cir. 1993).

<sup>35</sup> *Newman v. Metro. Pier & Exposition Auth.*, 962 F.2d 589, 591 (7th Cir. 1992).

<sup>36</sup> *Nat'l Hockey League*, 427 U.S. at 642.

<sup>37</sup> See *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 107 (2d Cir. 2002).

<sup>38</sup> *Id.* ("The sanction of an adverse inference may be appropriate in some cases involving the negligent destruction of evidence because each party should bear the risk of its own negligence.").

<sup>39</sup> *Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D. 68, 75 (S.D.N.Y. 1991).

<sup>40</sup> See *Jeffries v. Chicago Transit Auth.*, 770 F.2d 676, 681 (7th Cir. 1985) (finding that the destruction of documents through a business retention schedule did not impute any bad faith or consciousness of guilt where the destruction did not violate federal regulations and the defendant was not on notice that a lawsuit would be filed against it); see also *Lewy v. Remington Arms Co., Inc.*, 836 F.2d 1104 (8th Cir. 1988).

or should have known that the documents would become material at some point in the future then such documents should have been preserved.<sup>41</sup>

The court cautioned that “a corporation cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy.”<sup>42</sup>

Parties faced with litigation involving electronic discovery need to appreciate the unique challenges posed by ESI and make sure they are taking adequate steps to meet their preservation obligations. The consequences of failing to do so can be dire.

Courts have considerable latitude to fashion appropriate sanctions for spoliation of evidence, and FED. R. CIV. P. 37 “authorizes a panoply of sanctions for a

party’s failure to comply with the rules of discovery.”<sup>43</sup> The nature and severity of the sanction usually hinges on the culpability of the noncompliant party and any prejudice suffered by the other party as a result. Sanctions may be relatively mild, such as an order extending the discovery period, precluding the introduction of evidence or cross-examination on a subject,<sup>44</sup> or allowing additional or alternative discovery.<sup>45</sup> To ensure that a party does not benefit from its own discovery failings, courts may bar a party from introducing certain evidence at trial,<sup>46</sup> bar the testimony of particular witnesses at trial,<sup>47</sup> or preclude a party from introducing any evidence or argument pertaining to a specific topic.<sup>48</sup>

<sup>41</sup> Lewy, 836 F.2d at 1112 (citations omitted).

<sup>42</sup> *Id.*

<sup>43</sup> Residential Funding Corp., 306 F.3d at 101.

<sup>44</sup> Larson v. Bank One Corp., 2005 WL 4652509 (N.D. Ill. Aug. 18, 2005) (where the defendant breached its duty to preserve by failing to establish a “comprehensive document retention policy” and by failing to properly disseminate the policy to its employees, and conduct evinced “extraordinarily poor judgment” and “gross negligence” but not willfulness or bad faith, the magistrate recommended that the prejudice to the plaintiff could be remedied by precluding the defendant from cross-examining the plaintiff’s financial expert and by instructing the jury about the sanction).

<sup>45</sup> Crandall v. City and County of Denver, Colo., 2006 WL 2683754 (D. Colo. Sept. 19, 2006) (court denied motion for sanctions but allowed additional discovery, opining: “Mere existence of a document (in this case e-mail) destruction policy within a corporate entity, coupled with a failure to put a comprehensive ‘hold’ on that policy once the corporate entity becomes aware of litigation, does not suffice to justify a sanction absent some proof that, in fact, it is potentially relevant evidence that has been spoiled or destroyed.”); *see also* Streamline Capital LLC v. Hartford Cas. Ins. Co., 2004 WL 2663564 (S.D.N.Y. Nov. 19, 2004) (where key witnesses systematically deleted potentially relevant emails before and during litigation, the magistrate deferred decision on sanctions and ordered witnesses to consent to production of pertinent emails still available through their email service companies in order to determine, to the extent possible, the degree of prejudice the defendant suffered by virtue of the deletions); Renda Marine, Inc. v. U.S., 58 Fed. Cl. 57 (2003) (in view of the key player’s practice of deleting relevant email documents, which continued even after the lawsuit commenced, the court ordered the defendant to produce at its expense those back-up tapes that were created on and after the date on which the duty to preserve was triggered, and to provide access to the hard drive); Wiginton v. CB Richard Ellis, Inc., 2003 WL 22439865 (N.D. Ill. Oct. 27, 2003) (magistrate recommended that the plaintiff’s sanctions motion be denied without prejudice; the motion could be renewed if the plaintiff’s expert was able to discover relevant documents on backup tapes).

<sup>46</sup> *See, e.g.*, Thompson v. U.S. Dep’t of Hous. & Urban Dev., 219 F.R.D. 93 (D. Md. 2003) (defendant precluded from using any of the 80,000 e-mail records it belatedly produced).

<sup>47</sup> U.S. v. Philip Morris USA Inc., 327 F. Supp. 2d 21 (D.D.C. 2004) (court barred testimony from at least 11 witnesses who failed to comply with the court’s preservation order and the defendant’s own internal document retention program); Sheppard v. River Valley Fitness One, LP, 203 F.R.D. 56 (D.N.H. 2001) (where the defense counsel’s failure to produce computer records and to retain all drafts of settlement documents reflected lack of diligence rather than intentional effort to abuse discovery process, the court barred testimony of the witness and imposed \$500 in sanctions).

<sup>48</sup> *See, e.g.*, Serra Chevrolet, Inc. v. Gen. Motors Corp., No. CV-01-VEH-2682-S (N.D. Ala. May 20, 2005) (among other sanctions, the court prohibited GM from challenging any aspect of the plaintiff’s expert opinion on certain topics); *see also* In re LTV Steel Co., Inc., 307 B.R. 37, 2004 WL 547933 (Bankr. N.D. Ohio Jan. 6, 2004) (noting that the court would be within its discretion to dismiss the creditor’s claim because of the creditor’s repeated and willful failure to

Increasingly severe sanctions are likely when a party's discovery failings are grossly negligent, reckless, deliberate, or in bad faith. Courts may shift the burden of proof on a particular issue, forcing the defendant into the awkward position of having to disprove a claim asserted by the plaintiff.<sup>49</sup> Another possible evi-

dentiary sanction is an adverse inference instruction, which allows a jury to infer from the fact that a party destroyed certain evidence that the evidence, if available, would have been favorable to the party's opponent and harmful to the party who destroyed it.<sup>50</sup>

If the breach of a duty to preserve is particularly

---

comply with the debtor's discovery requests related to the central issue of the creditor's claim, the court instead barred the creditor from offering evidence or argument pertaining to the disputed portion of the claim); *Wilson v. Sundstrand Corp.*, 2003 WL 21961359 (N.D. Ill. Aug. 18, 2003) (as sanction for discovery abuse and tardy production of a "smoking gun" email, the court precluded the defendant from opposing the admission of various emails and records); *Deloach v. Philip Morris Co., Inc.*, 206 F.R.D. 568 (M.D.N.C. 2002) (where the defendant withheld computerized data and the defense expert subsequently used the data in a rebuttal report, the court allowed the plaintiffs the opportunity to respond to the defendants' rebuttal expert report, and ruled that the defendants would not be allowed an opportunity to reply to the plaintiffs' response to the withheld information).

<sup>49</sup> See, e.g., *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005) (for the defendant's numerous willful and grossly negligent discovery abuses, the court's sanctions included: (1) burden of proof on fraud issue shifted to the defendant, (2) court would read to jury a statement of facts recounting the defendant's duty to preserve evidence and its failure to do so, and such facts would be deemed conclusive, and (3) the defendant ordered to compensate the plaintiff for costs and fees associated with dispute).

<sup>50</sup> See, e.g., *Zubulake v. UBS Warburg, LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004) ("*Zubulake V*") (where the defendant acted willfully in destroying potentially relevant information, which resulted in the absence of such information or its tardy production, the court granted the plaintiff's motion for sanctions including adverse inference instruction and monetary sanctions); see also *In re Napster, Inc. Copyright Litig.*, 2006 WL 3050864 (N.D. Cal. Oct. 25, 2006) (adverse inference instruction and monetary sanctions imposed where the defendant acknowledged that its personnel routinely deleted emails without regard to whether the deleted emails were relevant to the litigation, but the behavior did not constitute a pattern of deliberately deceptive litigation practices and there was evidence that the actual number of emails lost was small); *Easton Sports, Inc. v. Warrior LaCrosse, Inc.*, 2006 WL 2811261 (E.D. Mich. Sept. 28, 2006) (adverse inference instruction recommended based in part on a key player's cancellation of his Yahoo email account since "[t]he inevitable, and fully foreseeable result of that contract termination was the loss of relevant evidence which would otherwise have been recoverable"); *3M Innovative Props. Co. v. Tomar Elecs.*, 2006 WL 2670038 (D. Minn. Sept. 18, 2006) (court affirmed the magistrate's report that recommended the imposition of sanctions, including an adverse inference instruction, based in part upon the defendant's failure to implement a legal hold); *Morgan v. U.S. Xpress, Inc.*, 2006 WL 1548029 (M.D. Ga. June 2, 2006) (personal injury plaintiff avoided summary judgment based in part on adverse inference allowed by the court for "questionable circumstances" surrounding the defendant's destruction of satellite positioning data); *Clark Constr. Group, Inc. v. City of Memphis*, 229 F.R.D. 131 (W.D. Tenn. 2005) (imposing rebuttable adverse inference based upon the city's grossly negligent failure to institute a litigation hold and consequent destruction of email printouts and relevant hardcopy documents); *E\*Trade Secs. LLC v. Deutsche Bank AG*, 230 F.R.D. 582 (D. Minn. 2005) (sanctions in the form of an adverse inference instruction and attorneys' fees imposed where a party committed spoliation by permanently erasing hard drives, failing to retain DVDs of relevant audio recordings, and failing to place an adequate litigation hold on email boxes while making no changes to its three-year retention policy for email backup tapes); *Broccoli v. Echostar Commc'ns Corp.*, 229 F.R.D. 506 (D. Md. 2005) (adverse inference instruction and monetary sanctions imposed where the defendant failed to suspend its "extraordinary email/document retention policy" which provided for automatic purging of emails after 21 days and complete deletion of all electronic files of former employees 30 days after their departure); *Paramount Pictures Corp. v. Davis*, 2006 WL 2092581 (E.D. Pa. July 26, 2006) (spoliation inference based on the defendant's wiping his hard drive clean of all data further supported the court's judgment in favor of the plaintiff after bench trial); *DaimlerChrysler Motors v. Bill Davis Racing, Inc.*, 2005 WL 3502172 (E.D. Mich. Dec. 22, 2005) (magistrate recommended an adverse inference instruction as a sanction for the defendant's negligent failure to institute a litigation hold which resulted in irretrievable loss of email messages through computer system's automatic deletion feature); *Hous. Rights Ctr. v. Sterling*, 2005 WL 3320739

flagrant, a court may strike a party's pleadings and enter judgment against it.<sup>51</sup> This is an extreme remedy which is imposed only where there has been willful and bad faith spoliation, and less drastic sanctions

cannot properly redress the wrongdoing. For example, several courts have imposed litigation-ending sanctions against parties who attempted to delete damaging evidence from their computers using special

---

(C.D. Cal. Mar. 2, 2005) (adverse inference instruction and monetary sanctions imposed where the defendants committed "egregious" discovery abuses, including: failure to institute or communicate a proper legal hold; failure to verify with appropriate personnel whether there was an email backup system; failure to search for documents; and "purposeful sluggishness" in taking steps to prevent destruction of evidence and in responding to discovery requests); *Mosaid Techs. Inc. v. Samsung Elecs. Co., Ltd.*, 348 F. Supp. 2d 332 (D.N.J. 2004) (finding the defendant's actions went "far beyond mere negligence, demonstrating knowing and intentional conduct that led to the nonproduction of all technical e-mails," the district court affirmed the spoliation inference jury instruction and monetary sanctions imposed by the magistrate); *Advantacare Health Partners, LP v. Access IV*, 2004 WL 1837997 (N.D. Cal. Aug. 17, 2004) (adverse inference instruction and monetary sanctions warranted where, in advance of a court-ordered inspection, the defendants deleted from their computers numerous electronic files which had been copied from a former employer's computer systems); *MasterCard Int'l v. Moulton*, 2004 WL 1393992 (S.D.N.Y. June 22, 2004) (although it found no bad faith in failure to preserve email since the defendants simply persevered in their normal document retention practices, the court ruled that the plaintiff would be allowed to prove the facts reflecting the non-retention of e-mail and argue to the trier of fact that this destruction of evidence, in addition to other proof offered at trial, warranted certain inferences); *Anderson v. Crossroads Capital Partners, LLC*, 2004 WL 256512 (D. Minn. Feb. 10, 2004) (adverse inference instruction imposed for the plaintiff's use of "Cyberscrub" data wiping software prior to a court-ordered inspection); *3M v. Pribyl*, 259 F.3d 587, 606 n.5 (7th Cir. 2001) (negative inference instruction warranted where six gigabytes of music were downloaded onto a hard drive the night before the computer was to be turned over for inspection); *Trigon Ins. Co. v. U.S.*, 204 F.R.D. 277 (E.D. Va. 2001) (adverse inference instruction imposed where the government had a duty to preserve correspondence between experts and consultants, including drafts of expert reports, and the destruction of such evidence was intentional).

<sup>51</sup> *Leon v. IDX Sys. Corp.*, 464 F.3d 951 (9th Cir. 2006) (affirming the trial court's dismissal of the plaintiff's claims and a \$65,000 sanction based on the plaintiff's deletion of 2,200 potentially relevant files from his IDX-issued laptop computer during pendency of litigation); *Plasse v. Tyco Elecs. Corp.*, 2006 WL 2623441 (D. Mass. Sept. 7, 2006) (where a forensic inspection showed evidence of deleted files and the plaintiff's explanations "verge[d] on the absurd," the court dismissed the complaint with prejudice and invited the defendant to submit an application for costs and attorneys' fees); *Ridge Chrysler Jeep, LLC v. Daimler Chrysler Servs. N. Am., LLC*, 2006 WL 2808158 (N.D. Ill. Sept. 6, 2006) (the plaintiff's false statements to the court and failure to preserve evidence warranted dismissal of the complaint); *Covucci v. Keane Consulting Group, Inc.*, 2006 WL 2004215 (Mass. Super. Ct. May 31, 2006) (dismissal of the complaint was the only appropriate sanction where the plaintiff intentionally and in bad faith destroyed evidence relating to the creation of "crucial" email and provided false and misleading testimony at deposition and at evidentiary hearing); *Krumwiede v. Brighton Assocs., L.L.C.*, 2006 WL 1308629 (N.D. Ill. May 8, 2006) (the plaintiff's willful and bad faith spoliation of evidence and "hide the ball" tactics warranted default judgment on counterclaims); *Magana v. Hyundai Motor Am.*, No. 00-2-00553-2 (Clark County, Wash. Super. Ct. Feb. 15, 2006) (default judgment was entered based upon Hyundai's misrepresentations and failure to produce evidence, reinstating the jury's earlier \$8 million damages award); *Metro. Opera Ass'n, Inc. v. Local 100, Hotel Employees & Rest. Employees Int'l Union*, 212 F.R.D. 178 (S.D.N.Y. 2003) (judgment entered in the plaintiff's favor on the issue of liability where the defendants failed to produce email and electronic documents and failed to preserve computer hard drives, among other discovery abuses); *In re Telxon Corp. Sec. Litig.*, 2004 WL 3192729 (N.D. Ohio July 16, 2004) (magistrate recommended an entry of default judgment on liability against PricewaterhouseCoopers, LLP, concluding that "PWC and/or its counsel engaged in deliberate fraud or was so recklessly indifferent to their responsibilities as a party to litigation that they failed to take the most basic steps to fulfill those responsibilities."); *QZO, Inc. v. Moyer*, 594 S.E.2d 541 (S.C. Ct. App. 2004) (trial court did not abuse its discretion in striking the defendant's answer and entering judgment for the plaintiff on the issue of liability where the defendant reformatted a computer's hard drive, effectively erasing any information the computer may have contained, a day before surrendering it for court ordered inspection); *Nartron Corp. v. Gen. Motors Corp.*, 2003 WL 1985261 (Mich. Ct. App. Apr. 29, 2003) (court dismissed the plaintiff's claims as discovery sanction after four-day evidentiary

wiping software bearing such names as “Evidence Eliminator” or “Data Eraser.”<sup>52</sup>

Destruction of evidence in a civil case or regulatory

investigation, if sufficiently egregious, may even lead to criminal charges against the spoliator. For example, at least one court has suggested that incarceration of a

---

hearing on alleged discovery abuses by the plaintiff, *e.g.*, delays in responding to discovery requests and attenuated and piecemeal production of altered/partially deleted database); *R.S. Creative, Inc. v. Creative Cotton, Ltd.*, 89 Cal. Rptr. 2d 353 (Cal. Ct. App. 1999) (trial court properly imposed terminating sanctions against the plaintiff for egregious discovery abuses, including the deletion of files from hard drives after the plaintiff stipulated that computers and diskettes would not be operated or touched until the defendants’ computer expert could examine them); *Century ML-Cable Corp. v. Carrillo*, 43 F. Supp. 2d 176 (D.P.R. 1998) (default judgment entered against party who willfully destroyed customer records and a laptop computer following a TRO prohibiting destruction of those items); *Long Island Diagnostic Imaging, P.C. v. Stony Brook Diagnostic Assocs.*, 728 N.Y.S.2d 781 (App. Div. 2001) (trial court erred in not dismissing the defendants’ counterclaim and third party complaint as sanction for spoliation of evidence—contrary to the court’s orders, the defendants purged databases and produced backup tapes that were compromised and unusable); *Crown-Life Ins. Co. v. Craig*, 995 F.2d 1376 (7th Cir. 1993) (court entered default judgment against an insurer on an agent’s counterclaim as sanction for an insurer’s willful failure to comply with discovery orders requiring the production of a relevant database); *Am. Bankers Ins. Co. of Fla. v. Caruth*, 786 S.W.2d 427 (Tex. App. 1990) (entry of default judgment on the issue of liability against an insurer for failure to produce computer data was not an abuse of discretion); *Computer Assoc. Int’l, Inc. v. Am. Fundware, Inc.*, 133 F.R.D. 166 (D. Colo. 1990) (the defendant’s destruction of source code warranted a default judgment on the issue of liability); *Wm. T. Thompson Co. v. Gen. Nutrition Corp., Inc.*, 593 F. Supp. 1443 (C.D. Cal. 1984) (court imposed the “ultimate” sanction of striking the defendant’s answer and entering a default judgment, and imposed monetary sanctions of \$453,312.56 for the plaintiff’s fees and costs associated with the discovery abuses); *see also In re Quintus Corp.*, 2006 WL 3072982 (Bankr. D. Del. Oct. 27, 2006) (court entered \$1,888,410 judgment in favor of a bankruptcy trustee as sanction for the adverse party’s destruction of crucial financial records).

<sup>52</sup> *Arista Records, LLC v. Tschirhart*, 2006 WL 2728927 (W.D. Tex. Aug. 23, 2006) (imposing sanction of default judgment entered where forensic evidence showed that the defendant deliberately used “wiping” software to permanently remove data from her hard drive, the court stated: “The sanction in the present case is to deter other defendants in similar cases from attempting to destroy or conceal evidence of their wrongdoing.”); *Elec. Funds Solutions v. Murphy*, 36 Cal. Rptr. 3d 663 (Ct. App. 2005) (trial court properly struck the defendants’ answer as a discovery sanction for discovery abuse that included misrepresentations to the court, failure to comply with discovery orders and intentional destruction of evidence through the use of “Data Eraser” software; however, compensatory and punitive damage awards totaling over \$24 million would be vacated and remanded since the complaint that sought damages in excess of \$50,000 failed to put the defendants on notice of their maximum potential liability); *Comm’n Center, Inc. v. Hewitt*, Civ. No. S-03-1968 WBS KJM, 2005 WL 3277983 (E.D. Cal. Apr. 5, 2005) (where the defendants used “Evidence Eliminator” software on hard drives while under a court order to produce mirror images of such drives, the magistrate recommended that the defendants’ answer be stricken and default entered against the defendants on 8 of 10 causes of action; the magistrate also ordered the defendants to pay the plaintiff’s attorneys’ fees and expenses in connection with the motion amounting to \$145,812); *DirecTV, Inc. v. Borow*, 2005 WL 43261 (N.D. Ill. Jan. 6, 2005) (granting summary judgment against the defendant on the issue of liability, the court afforded the plaintiff an adverse inference based upon the defendant’s use of “Evidence Eliminator” software to erase evidence requested by the plaintiff from his computer); *Kucala Enters., Ltd. v. Auto Wax Co., Inc.*, 2003 WL 21230605 (N.D. Ill. May 27, 2003) (magistrate recommended that a competitor’s suit against a patent holder be dismissed with prejudice as sanction for egregious discovery abuse, which included the use of “Evidence Eliminator” software to delete documents from a computer in advance of a court-ordered inspection); *Kucala Enters., Ltd. v. Auto Wax Co., Inc.*, 2003 WL 22433095 (N.D. Ill. Oct. 27, 2003) (district judge adopted all the magistrate’s findings and recommendations, with the exception that the plaintiff would be allowed to proceed on a claim of non-infringement and to defend an infringement counterclaim on the condition that all discovery be made “forthwith”). *But see Anderson v. Crossroads Capital Partners, LLC*, 2004 WL 256512 (D. Minn. Feb. 10, 2004) (the plaintiff’s use of “Cyberscrub” data wiping software prior to a court-ordered inspection of her computer, after agreeing on the record that she would not purge her hard drive or delete any documents, and her misrepresentations about the age of the hard drive were not sufficiently egregious to warrant dismissal, but did warrant an adverse inference instruction).

party's CEO might be an appropriate sanction for civil discovery misconduct.<sup>53</sup> In the realm of regulatory investigations in the securities field, the *Arthur Andersen*<sup>54</sup> and *Frank Quattrone*<sup>55</sup> criminal cases illustrate that criminal charges may follow a party's wrongful destruction of relevant evidence.

Courts commonly award monetary sanctions against a party that has breached its duty to preserve. The court may hold the spoliator in contempt<sup>56</sup> or require it to pay a fine to the adverse party<sup>57</sup> or directly to

the court.<sup>58</sup> More frequently, courts will award the injured party its reasonable costs, expert fees, and attorneys' fees incurred as a result of the discovery abuse.<sup>59</sup>

Even where no sanctions are imposed, mistakes and miscommunications over preservation duties can be costly. Discovery motion practice can throw a case off course, diverting the parties' energies away from the merits of the litigation and consuming resources—including valuable court time—that would be better spent addressing the parties' substantive claims.<sup>60</sup>

---

<sup>53</sup> In *Cooney v. Beverly Enter., Inc.*, No. CV 2003-1049-3 slip op. (Saline County Cir. Ct., Ark. June 15, 2005), the court found the defendants in contempt of the court's prior order compelling discovery. In addition to ordering the defendants to bring themselves into full compliance and pay the plaintiffs' attorneys' fees, the court stated that it would, on its own suggestion, take under advisement what additional sanctions, if any, should be imposed on the defendants, including whether the CEO and others should be incarcerated.

<sup>54</sup> *U.S. v. Arthur Andersen, LLP*, 374 F.3d 281 (5th Cir. 2004). In this case, the Fifth Circuit affirmed the conviction of Arthur Andersen for obstructing an official proceeding of the SEC based upon evidence that, in order to protect the firm and the firm's largest single account (Enron), Arthur Andersen ordered a mass destruction of documents to keep them from the hands of the SEC. During trial, Arthur Andersen unsuccessfully defended the destruction of documents as a legitimate practice under its document retention policies. The United States Supreme Court subsequently reversed the conviction in *Arthur Andersen, LLP v. U.S.*, 544 U.S. 696 (2005), in part because the jury instructions failed to convey the requisite consciousness of wrongdoing. The case has been remanded for further proceedings.

<sup>55</sup> *U.S. v. Quattrone*, 441 F.3d 153 (2d Cir. 2006). At trial, Frank Quattrone, an investment banker, was convicted for obstruction of justice and witness tampering in connection with investigations conducted by the SEC, NASD and a grand jury, and sentenced to 18 months' imprisonment. Among other things, Mr. Quattrone sent an email to bankers in his group that "strongly advise[d]" them to comply with the firm's document destruction policies at a time when he knew or should have known about the investigations. Although the Second Circuit held that erroneous jury instructions required remand, it concluded that the evidence was sufficient to support the convictions).

<sup>56</sup> See, e.g., *Landmark Legal Found. v. EPA*, 272 F. Supp. 2d 70 (D.D.C. 2003) (EPA held in civil contempt for violating a preliminary injunction by reformatting hard drives and erasing or overwriting backup tapes containing potentially responsive email and ordered to pay the plaintiffs' reasonable attorneys' fees incurred as a result of EPA's contumacious conduct).

<sup>57</sup> *Procter & Gamble Co. v. Haugen*, 179 F.R.D. 622 (D. Utah 1998) (the plaintiff was ordered to pay the defendant \$10,000 for failing to preserve or search the email of five individuals (\$2,000 for each individual)).

<sup>58</sup> See, e.g., *U.S. v. Philip Morris USA Inc.*, 327 F. Supp. 2d 21 (D.D.C. 2004) (court sanctioned the defendant \$2,750,000 to be paid to court registry for its failure to follow the court's preservation order); see also *Danis v. USN Commc'ns, Inc.*, 2000 WL 1694325 (N.D. Ill. Oct. 20, 2000) (magistrate recommended that the defendant CEO be sanctioned \$10,000 for document preservation failings, to be paid to court registry).

<sup>59</sup> *Consol. Aluminum Corp. v. Alcoa, Inc.*, 2006 WL 2583308 (M.D. La. July 19, 2006) (for negligent failure to preserve electronic evidence, the defendant was ordered to pay reasonable attorneys' fees incurred by the plaintiff in bringing sanctions motion and investigating and attempting to obtain discovery at issue and costs of re-deposing certain witnesses); *Vela v. Wagner & Brown, Ltd.*, 2006 WL 1684191 (Tex. App. June 21, 2006) (affirming \$75,000 sanctions award based upon the defendant's failure to properly preserve and timely produce its expert's underlying computer data); *Invision Media Commc'ns, Inc. v. Fed. Ins. Co.*, 2004 WL 396037 (S.D.N.Y. Mar. 2, 2004); *Nat'l Ass'n of Radiation Survivors v. Turnage*, 115 F.R.D. 543 (N.D. Cal. 1987) (the defendant was ordered to pay monetary sanctions—\$105,000 to the plaintiffs and \$15,000 to the clerk of court).

<sup>60</sup> See, e.g., *Danis v. USN Commc'ns, Inc.*, 2000 WL 1694325 (N.D. Ill. Oct. 20, 2000) (the parties collectively spent over \$1.5 million litigating sanctions issues alone).

## Unique Preservation Issues Presented by Electronic Data

The preservation of ESI presents some unique challenges when compared to traditional, “hard copy” data. These challenges arise in large part because of a few areas in which ESI differs dramatically from hard copy data: volume, organization, and content.

An estimated 92 percent of new information created today is electronic,<sup>61</sup> and much of that is never reduced to printed form. As storage of electronic information has become virtually effortless for computer users and increasingly less expensive, many companies are finding that they possess vast quantities of electronic documents unlike anything they would have accumulated in the paper world. An employee may easily store the equivalent of millions of pages on a single hard drive or on the company’s network server.

In addition to the increased volume of information stored electronically, the way in which electronic information is organized often poses additional challenges. In contrast to paper records, which are typically sorted by subject matter and require some conscious decision-making and physical effort to organize and file, electronic information is not necessarily stored in any rational order. Employees may simply move material into one huge folder, without taking the time or effort to sort it in any meaningful way. Further, there are many more potential locations and sources of electronic material than there are for paper records. Depending on a company’s computer network structure and the employee’s own computer usage practices, an employee may save electronic information on the hard drives of his desktop computer, home computer and/or laptop, on the company’s file servers, and on floppy disks or CD-ROMs.

Adding to the problem, ESI is often retained without regard to its relevance to the company’s ongoing business. Some employees send and receive hundreds of emails each week. Although many of these emails have no lasting business value, the employee may keep them all by default, because doing so takes significantly less time and effort than identifying the truly

significant emails and storing them in a coherent fashion. On the other hand, companies may employ janitorial systems to automatically delete email after a certain time period, which could not happen in a paper world. Although this helps reduce the volume of information being retained, the automated manner in which it happens results in a decision being made about the retention of a document without regard to its content.

In addition, electronic documents may contain information that “disappears” when the file is converted to hard copy unless separately captured on conversion, such as hidden comments viewable only in the electronic version of a document, hidden columns in a spreadsheet, or the metadata attached to an electronic document.<sup>62</sup> Computer systems may lose, alter, or destroy information as part of their routine operations, making the risk of losing information significantly greater than it would be in the context of paper documents. It may be difficult, or even impossible, to interrupt or suspend routine operations of computer systems to isolate and preserve discrete parts of the information they overwrite, delete, or update on an ongoing basis, without creating other problems for the overall system. Suspension of these features may also make discovery more costly and time consuming by causing a greater accumulation of duplicative and irrelevant data that must be reviewed. In this environment, defining the scope of a company’s duty to preserve evidence, and ensuring that that duty is satisfied, becomes especially challenging.

The drafters of the 2006 e-discovery amendments to the Federal Rules of Civil Procedure recognized these unique challenges. The new Rule 37(f) responds to a distinctive and necessary feature of computer systems—the recycling, overwriting, and alteration of ESI that attends normal use. It provides some protection from sanctions for a party’s failure to preserve and produce certain electronic material in discovery:

Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information

<sup>61</sup> See Lyman, Peter and Hal R. Varian, *How Much Information?* 2003, available at <http://www.sims.berkeley.edu/how-much-info-2003>.

<sup>62</sup> Metadata includes both visible information, such as author, recipient, and subject line of an email, as well as hidden data, such as last saved date and creator.

lost as a result of the routine, good-faith operation of an electronic information system.<sup>63</sup>

Although this “safe harbor” provision is a welcome advance, it provides no bright lines or quick answers. Whether a party is able to take advantage of this provision to avoid sanctions in a specific case will depend upon the particulars of the case. The effect that this new rule will have on litigants’ preservation efforts, if any, remains to be seen.

## **Records Management—Document Retention and Destruction Policies**

### *Companies Should Consider Implementing and Following a Document Retention Policy*

A document retention and destruction policy is a set of guidelines instituted by a company to control the volume of material it retains and to organize how records are stored, retrieved, and purged. An effective policy increases a company’s ability to meet its preservation obligations and respond to requests for documents while decreasing its costs in doing so.

Because there is no such thing as a “standard” company or organization, there is no such thing as a “standard” document retention policy. Every policy will be unique, and will depend on the culture, nature, and needs of the company for which it is developed.<sup>64</sup> Successfully implementing a policy consistent with individual company practices allows a company to more effectively:

- Comply with all relevant law by providing mechanisms for preserving those documents it is required to keep pursuant to law or regulation.<sup>65</sup>
- Allow for the destruction of documents that are not

required to be kept and for which there is no reason to keep.

- Retain useful corporate information by providing mechanisms to identify and keep information that has a business purpose.
- Reduce the volume of storage devoted to outdated, unnecessary, or duplicative information.
- Ease the retrieval of documents and other information when it is necessary.
- Educate employees about the importance of document retention and destruction.
- Prepare for document retention obligations arising from actual or potential litigation.

### *Considerations for a Reasonable Document Retention Policy*

“The hallmark of an organization’s information and records management policies should be reasonableness.”<sup>66</sup> Stated another way, the approach taken toward retaining documents and data should be reasonable after considering facts and circumstances specific to the actual documents.<sup>67</sup> For example, “[a] three year retention policy may be sufficient for documents such as appointment books or telephone messages, but inadequate for documents such as customer complaints.”<sup>68</sup>

The nature of the company’s business needs should also be considered. Given the ubiquity of computers today, a records retention policy should specifically address ESI.<sup>69</sup> However, retention decisions should be based on content—not form, and retention periods should be driven by the information contained in the document—not whether it is in hard copy or electronic form.<sup>70</sup>

The law is well settled that document destruction and retention policies are not only an accept-

<sup>63</sup> FED. R. CIV. P. 37(f).

<sup>64</sup> THE SEDONA GUIDELINES FOR MANAGING INFORMATION AND RECORDS IN THE ELECTRONIC AGE, Guideline 2, comment 2.c. at 18 (The Sedona Conference®, July 2005) [hereinafter THE SEDONA GUIDELINES].

<sup>65</sup> *Id.*

<sup>66</sup> *Id.* at Guideline 1, Comment 1.b. at 14.

<sup>67</sup> *Lewy v. Remington Arms Co., Inc.*, 836 F.2d 1104, 1112 (8th Cir. 1988).

<sup>68</sup> *Id.*

<sup>69</sup> For a broad overview of electronic records management principles and suggested guidelines, see THE SEDONA GUIDELINES.

<sup>70</sup> See Gregory S. McCurdy & Martha J. Dawson, *Are Instant Messages Discoverable? Is This Digital Medium More Like E-Mails or Phone Calls?*, *The National Law Journal*, June 7, 2004, §1, col. 2, available at <http://www.prestongates.com/publications/article.asp?pubID=479> [registration required].

able means of controlling corporate data, but are expected.<sup>71</sup> A reasonable policy does not require that everything be maintained,<sup>72</sup> and clearly would be of little use if it did. Document destruction is an equally important component of all good retention policies. Even in the context of litigation, courts have recognized that companies must be allowed to dispose of some data.<sup>73</sup> As long as a mechanism—such as a legal hold notice—is put in place to ensure that documents potentially relevant to litigation are retained, a company may dispose of irrelevant documents.

A reasonable policy should also address the potential storage of corporate documents off of the corporate computer network. Today's growing culture of telecommuting raises the risk that documents are being stored on laptops and home computers outside the reach of any scheduled retention and destruction processes. For organizations where this is an issue, an effective retention policy should specifically address this possibility. This can be done by setting protocols to ensure that necessary documents are retained—*e.g.*, by requiring user to save such information on a regular basis to a corporate server.

Another crucial element of a reasonable retention

policy is that the guidelines it sets for the retention or destruction of information are based on objective, neutral criteria. As a starting point, all retention and destruction policies must comply with any federal, state, or local laws and regulations concerning the retention of specific materials. For other materials, document retention policies must not be implemented with the goal of selectively deleting “bad” documents. When a party has destroyed relevant evidence through its adherence to a document retention policy, and spoliation is alleged, a court may consider whether the document retention policy was instituted in bad faith.<sup>74</sup> If it appears that a retention policy was created or implemented solely for gaining a tactical advantage in litigation, a court will closely scrutinize the timing and development of the party's policy.<sup>75</sup> On the other hand, a consistently implemented policy may protect a company against claims of selective document destruction.<sup>76</sup>

The most effective way to prevent claims of bad faith regarding the administration of a document retention policy is to use it regularly and consistently. This means that once a reasonable retention policy has been adopted, it needs to be communicated,<sup>77</sup>

<sup>71</sup> Arthur Andersen, LLP v. U.S., 544 U.S. 696, 704 (2005); Remington Arms, 836 F.2d at 1112.

<sup>72</sup> THE SEDONA GUIDELINES, Guideline 1, Comment 1.c. at 15; *see also* Zubulake IV, 220 F.R.D. at 217.

<sup>73</sup> *Id.*

<sup>74</sup> Remington Arms, 836 F.2d at 1112.

<sup>75</sup> *See* Rambus, Inc. v. Infineon Techs. AG, 220 F.R.D. 264 (E.D. Va. 2004) (where the plaintiff developed both its patent litigation strategy and document retention program at the same time, the court ordered the plaintiff to produce privileged documents relating to the creation, preparation, or scope of the document retention policy for *in camera* review); Samsung Elecs. Co., Ltd. v. Rambus, Inc., 439 F. Supp. 2d 524 (E.D. Va. 2006) (the plaintiff developed its document retention policy after it reasonably anticipated litigation and “the program was implemented principally to rid the company of discoverable documents at a time when it anticipated litigation”); *see also* Rambus, Inc. v. Infineon Techs. AG, 222 F.R.D. 280 (E.D. Va. 2004) (based on *in camera* review, the court granted the defendant's motion to compel based on the crime/fraud exception to the attorney-client privilege, ordered production of other documents on the same subject matter, and further ruled that discovery would be allowed regarding documents produced and on the issue of sanctions). *But see* Hynix Semiconductor, Inc. v. Rambus, Inc., No. C-00-20905 RMW slip op. (N.D. Cal. Jan. 4, 2006) (after bench trial, the court concluded that dismissal of Rambus' patent infringement claims was not warranted under the unclean hands defense, since Rambus' adoption and implementation of a document retention policy was a “permissible business decision” and “shred days” did not constitute unlawful spoliation).

<sup>76</sup> *See* Renda Marine, Inc. v. U.S., 58 Fed. Cl. 57, 61 n.4 (2003) (“[t]he existence of the policy could bear on the question of the subjective good faith of persons operating under the policy and in compliance with it.”).

<sup>77</sup> *See, e.g.*, In re Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598 (D.N.J. 1997) (an insurer's “haphazard and uncoordinated approach to document retention” warranted an adverse inference instruction and \$1 million sanction).

consistently implemented,<sup>78</sup> and enforced. Success is most likely when senior management is brought on board early and demonstrates a commitment to the implementation and enforcement of the policy. Successful implementation requires that all employees understand the policy and its importance to the company. To ensure this, a company may want to consider a mandatory training program, as well as provide employees with ongoing resources and incentives to facilitate participation. Reminders sent at regular, pre-determined intervals might also be a good idea. Further, the oversight of responsible personnel, such as records managers and information system administrators, can help ensure that the records retention program is consistently and uniformly applied. Finally, there should be some mechanism to verify that employees are following the policy.

All the steps involved in drafting, implementing, and enforcing a retention policy and schedule should be well documented.<sup>79</sup> Such documentation is inval-

able to defending later charges of willful or bad faith document destruction.

### *Legal Hold Notices as a Best Practice of Document Retention*

Regardless of how a document retention policy is ultimately designed, it is important that it provide for the suspension of document destruction and lay out the processes with which to preserve documents potentially at issue in any litigation. A company should consider having the retention policy include a “Discovery Response Plan for Litigation” that outlines the specific steps for implementing a legal hold system for actual or “probable” litigation, as discussed below. The policy should lay out the specific steps necessary to suspend the destruction of documents and identify specific personnel responsible for overseeing these actions.<sup>80</sup> As part of a records retention program, companies should consider having a procedure to identify potential disputes and protect the corresponding ESI.<sup>81</sup> “A corpo-

---

<sup>78</sup> See, e.g., *Carlucci v. Piper Aircraft Corp.*, 102 F.R.D. 472 (S.D. Fla. 1984) (court found that the defendant destroyed relevant documents with the intention of preventing them from being produced in litigation and entered default judgment as sanction where the defendant “utterly failed” to show that its document retention policy was actually implemented in any consistent manner); see also *U.S. v. Philip Morris USA Inc.*, 327 F. Supp. 2d 21 (D.D.C. 2004) (finding it “astounding” that the defendant’s employees failed to follow the court’s preservation order and the defendant’s own document retention policies, the court imposed a monetary sanction of \$2,750,000 and barred testimony from at least 11 witnesses who failed to comply with the defendant’s document retention program).

<sup>79</sup> See, e.g., cases involving *Rambus, Inc.* and its implementation of a records retention policy, *supra* note 75.

<sup>80</sup> See THE SEDONA GUIDELINES, Guideline 5, at 42.

<sup>81</sup> See, e.g., *Zubulake V.*, 229 F.R.D. 422; *Danis v. USN Commc’ns, Inc.*, 2000 WL 1694325 (N.D. Ill. Oct. 20, 2000); *Metro. Opera Ass’n, Inc. v. Local 100, Hotel Employees & Rest. Employees Int’l Union*, 212 F.R.D. 178 (S.D.N.Y. 2003); see also *Broccoli v. Echostar Commc’ns Corp.*, 229 F.R.D. 506 (D. Md. 2005) (sanctions imposed where the defendant failed to suspend its “extraordinary email/document retention policy” which provided for automatic purging of emails after 21 days and complete deletion of all electronic files of former employees 30 days after their departure); *DaimlerChrysler Motors v. Bill Davis Racing, Inc.*, 2005 WL 3502172 (E.D. Mich. Dec. 22, 2005) (where email messages were irretrievably lost through the defendant’s computer system’s automatic deletion feature, the magistrate recommended an adverse inference instruction as sanction for the defendant’s negligent failure to institute a legal hold); *In re Old Banc One S’holders Sec. Litig.*, 2005 WL 3372783 (N.D. Ill. Dec. 8, 2005) (the defendant was barred from cross-examining the plaintiffs’ expert as sanction for its non-production of underlying financial data resulting from its negligent failure to institute and disseminate a litigation hold); *E\*Trade Secs. LLC v. Deutsche Bank AG*, 230 F.R.D. 582 (D. Minn. 2005) (sanctions in the form of an adverse inference instruction and attorneys’ fees imposed where a party committed spoliation by failing to place an adequate litigation hold on email accounts while making no changes to its three-year retention policy for email backup tapes); *Hous. Rights Ctr. v. Sterling*, 2005 WL 3320739 (C.D. Cal. Mar. 2, 2005) (court granted a motion for adverse inference instruction and monetary sanctions where the defendants committed “egregious” discovery abuses, including: failure to institute or communicate a proper legal hold; failure to verify with appropriate personnel whether there was an email backup system; failure to search for documents; and “purposeful sluggishness” in taking steps to prevent destruction of evidence and in responding to discovery requests).

ration cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy.<sup>82</sup> A records retention policy that is inconsistent with a party's preservation obligations in litigation does not operate to excuse the party's failure to respond to discovery.<sup>83</sup> However, "[t]he existence of the policy could bear on the question of the subjective good faith of persons operating under the policy and in compliance with it."<sup>84</sup>

Additionally, the safe harbor provision under amended Rule 37(f) applies only if a computer system was operated in "good faith." The committee notes state that the existence of a preservation obligation may play a role in determining whether or not the operation was in good faith, and that "[g]ood 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."

### *Retention Considerations for Disaster Recovery Systems*

Most businesses adopt some type of disaster recovery process to address legitimate concerns about keeping a business up and running in the event of a catastrophic disaster. These types of disasters can be natural (floods, fires, earthquakes) or technological (full server hardware failures). A common method of providing disaster recovery protection is through the use of backup tapes. As a general rule, backup tapes should only be maintained long enough to provide adequate recovery from a disaster. Problems arise when tapes are instead used as routine data archive depositories, in place of good document management practices, or saved simply because an IT person wants to save everything possible. Tapes are also problematic when maintained in large numbers for indefinite periods of time for no real business purpose. To understand why this can be such a problem, it is important to understand how backup tapes work.<sup>85</sup>

Typically, backup tapes record a snapshot of an entire server at the time the tape is made. They do not copy files in any organized fashion and to access a specific file on any given tape, the entire tape must be restored. If a document is saved on a server that is routinely backed up, it is backed up each time a tape is made. If tapes are not recycled or overwritten and new tapes are used each time, multiple copies of the same document will be saved on each subsequent tape. If the document has been edited in any way between backup cycles, slightly different copies of the same document will be saved. Given the amount of data most tapes are capable of storing, data duplication quickly becomes an enormous obstacle if and when the relevance of any material on those tapes comes into question or documents need to be reviewed.

Under the recent revisions to the Federal Rules of Civil Procedure, disaster recovery systems should be treated as "not reasonably accessible." FED. R. CIV. P. 26(b)(2) establishes a two-tiered approach to the production of ESI, differentiating between information that is reasonably accessible and that which is not. A responding party need not produce ESI from sources that it identifies as not reasonably accessible because of undue burden or cost. If the requesting party moves to compel discovery of such information, the responding party would be required to demonstrate undue burden or cost. Once that showing is made, a court may order discovery only for good cause, subject to the provisions of FED. R. CIV. P. 26(b)(2)(C).<sup>86</sup>

For all of the foregoing reasons, companies should consider taking a close look at their disaster recovery policies and consider including a procedure for handling this media under their document retention policy. The company should make decisions about the number of tapes maintained and the length of time they are kept. Frequently, disaster recovery retention is decided on an ad hoc basis, inconsistently or not at all. This can cause miscommunication with outside parties, including the court, regarding what is being preserved, and create serious problems in litigation. Ultimately, a com-

<sup>82</sup> *Lewy v. Remington Arms Co., Inc.*, 836 F.2d 1104, 1112 (8th Cir. 1988).

<sup>83</sup> *Renda Marine, Inc. v. U.S.*, 58 Fed. Cl. 57, 61 (2003).

<sup>84</sup> *Id.* at 61 n.4.

<sup>85</sup> See generally <http://www.emaglink.com/tape-facts.htm>.

<sup>86</sup> These provisions were previously located at FED. R. CIV. P. 26(b)(2)(i), (ii), and (iii).

pany should consider rotating and recycling tapes on the shortest schedule possible. “Absent a legal requirement to the contrary, companies may recycle or destroy hardware or media that contain data retained for business continuation or disaster recovery purposes.”<sup>87</sup>

## Legal Hold Notices

When the duty to preserve documents arises, counsel should immediately work with the client to establish an appropriate document preservation protocol. A company’s document retention policy may need to be suspended, at least in part. The most common method of assuring the preservation of documents for litigation is to put a legal hold notice in place.

### *Scope of the Legal Hold Notice*

How does counsel determine the scope of the legal hold notice? Essentially it comes down to determining the likely sources of relevant documents. There are two main questions to answer to identify sources of relevant documents: (1) Who has the documents? and (2) Where do the documents physically reside?

### Identifying Key Players

The duty to preserve ESI begins with the identification of the key players—the employees most likely to have potentially relevant documents.<sup>88</sup> The key players are the employees who created or received documents that may support or refute the claims by the parties or any third parties.<sup>89</sup> Counsel should use reasonable discretion when deciding who is a key player; not every employee is necessarily a key player, even though some relevant documents may have been distributed company-wide.

Placing employees under a legal hold notice does not necessarily mean that their documents will be collected and reviewed. The purpose of identifying key employees at the early stage of litigation is to cast a broad net to meet the duty to preserve relevant evidence. The list of employees whose documents will be collected and reviewed can often be narrowed

once the nature and scope of the case is more clearly defined, after the actual requests for production of documents have been served, after responses and objections to the requests have been formulated, and possibly through the meet and confer process. On the other hand, based on the requests for production, the key employees that are identified at the early stage may turn out to be insufficient to meet the company’s discovery obligations, and additional employees may need to be placed under a legal hold notice. A re-evaluation may be necessary if the complaint is amended, additional requests are served, a cross-complaint is served, or parties are added to the litigation.

It is often helpful to utilize interviews or questionnaires as part of an iterative process to identify key players. Personal interviews or form questionnaires sent out by litigation counsel can help narrow the field of key players whose documents should be preserved. These same devices may often serve to identify alternate sources not previously considered, while ruling out key players which counsel might otherwise have had to place under legal hold notice. They may also serve to educate counsel about internal issues not easily discoverable through document review, such as internal product code names, organizational reporting relationships, or the potential of sensitive business, personal, or privileged information residing in certain files. A questionnaire also serves to document the process of determining whose documents will be preserved.<sup>90</sup> Typical questions could address individual reporting relationships within the company hierarchy, job history descriptions, involvement with the subject matter at issue in the case, and individual data retention habits.

### Location of Relevant Documents

Counsel should work with the information technology (“IT”) department to determine the types of systems utilized by the company that could contain relevant ESI. Counsel should consider addressing these questions to the information technology department:

- Document Management Systems

<sup>87</sup> THE SEDONA GUIDELINES, Guideline 3, Comment 3.d. at 28.

<sup>88</sup> Zubulake IV, 220 F.R.D. 212.

<sup>89</sup> FED. R. CIV. P. 26(a)(1)(A) and (b)(1).

<sup>90</sup> This documentation would be very helpful to prepare for a Rule 26(f) conference or Rule 30(b)(6) deposition.

- What email server system, including server software, do they use?
- What types of applications do they use?
- Do they save documents to network file shares?
- Do they use internal websites?
- Janitorial Programs
  - Do they use any programs that automatically delete email or other documents after a certain number of days, or when the volume reaches a certain size?
  - On what criteria is the automated deletion based?
  - What is required to disable such programs for specific individuals or locations?
- Disaster Recovery Systems
  - What are their disaster recovery policies for email servers?
  - What are their disaster recovery policies for other file servers?
  - What is the recycle period?
- Other Communication Tools
  - Do they employ technology that saves voicemail electronically?
  - Do the employees regularly use instant messaging programs to communicate?
  - What, if any, online collaboration tools are used by employees?

Electronic documents may be physically located in a wide variety of locations. The following are all potential sources that counsel may wish to consider for preservation:

- Databases
- Networks
- Computer systems
- Servers
- Hard drives (including portable Hard Disk Drives (HDDs))
- Archives
- Disaster recovery media
- Storage Media: DVDs, CDs, Floppy discs, Zip discs, Jazz discs, Tapes, Cartridges, *etc.*

- Laptops
- Personal Computers
- Internet Data
- Personal Digital Assistants (PDAs) including Palm, Blackberry, Cellular phone, Table PC, *etc.*

Additionally, many companies routinely move employees from office to office and computer to computer. It is important to investigate whether data belonging to a relevant custodian may still exist on a computer being used by a non-custodian. If a company does not have a standard protocol for wiping computer drives clean for each subsequent employee, data for relevant custodians may exist on multiple computers. Likewise, counsel may be accidentally collecting documents belonging to a non-custodian that exist on a custodian's computer.

Even when company policy requires custodians to store data in a centralized location, many will still store materials on their hard drive. Do not rely on representations such as "our employees are not allowed to store materials on their hard drives" or "employees do not know how to change their default storage options" when preserving documents. It is important to investigate all potential storage options, even those considered unlikely by IT personnel.

Counsel needs to become familiar with the client's computer systems and policies. The new federal rules require an attorney to be able to explain the company's systems, and the potentially relevant documents they contain, in the meet and confer conference required under the amended Rule 26(f). Counsel should understand any applicable records retention policies and disaster recovery protocols in place. Counsel should consider informing the IT department about the need to preserve relevant electronic evidence and work with them to ensure that existing data is preserved in accordance with the client's discovery obligations.<sup>91</sup> This point underscores the importance of understanding the client's computer systems and its protocols for electronic data management.<sup>92</sup>

<sup>91</sup> See, e.g., *DaimlerChrysler Motors v. Bill Davis Racing, Inc.*, 2005 WL 3502172 (E.D. Mich. Dec. 22, 2005) (where email messages were irretrievably lost through the defendant's computer system's automatic deletion feature, the magistrate recommended an adverse inference instruction as sanction for the defendant's negligent failure to institute legal hold); *E\*Trade Secs. LLC v. Deutsche Bank AG*, 230 F.R.D. 582 (D. Minn. 2005) (where a party committed spoliation by permanently erasing hard drives, failing to retain DVDs of relevant audio recordings, and failing to place adequate litigation hold on email accounts while making no changes to its three-year retention policy for email backup tapes,

Counsel should consider meeting with the employees who actually oversee these systems. Counsel should be cautious about relying on the representations of individuals who are not fully engaged with the corporate computer systems as to where, how, and for how long documents are stored, but should additionally confirm with the staff in charge of those systems. Counsel should be sure they actually understand what IT personnel are telling them. Computer jargon is easily misinterpreted. It is important for counsel not to assume they understand what is being represented without asking the follow up questions necessary to clarify the overall picture in a language that minimizes chances for error.<sup>93</sup>

Counsel also needs to consider possible sources of potentially relevant documents that are not directly controlled or maintained by particular employees, such as file shares, internal websites, databases, and any other shared or collaborative environment which has ESI.<sup>94</sup> Just as counsel should keep detailed records of their decisions regarding who was considered for

legal holds, including any decisions regarding employees who were determined not appropriate for legal holds, counsel should keep such records regarding non-employee sources of ESI.

### *Implementing a Legal Hold Notice*

Counsel should consider the proper means of communication for the company's culture. In many companies, email is the most appropriate means to convey the legal hold notice. In some companies, a memo circulated in hardcopy may be more effective. No matter what method is chosen, counsel should implement the legal hold notice through a written communication, and the employees placed under legal hold should be individually identified (*i.e.*, do not send a legal hold to an email distribution list or a memo to "department heads"). The notice should be sent by the legal department and preferably by a senior member of that department.<sup>95</sup>

Counsel also needs to meet with the information technology staff to make sure the documents of the

---

the district court adopted the magistrate's recommendation to impose sanctions in the form of an adverse inference instruction and attorneys' fees); *Hous. Rights Ctr. v. Sterling*, 2005 WL 3320739 (C.D. Cal. Mar. 2, 2005) (adverse inference instruction and monetary sanctions imposed where the defendants committed "egregious" discovery abuses, including: failure to institute or communicate a proper legal hold; failure to verify with appropriate personnel whether there was an email backup system; failure to search for documents; and "purposeful sluggishness" in taking steps to prevent destruction of evidence and in responding to discovery requests); *Danis v. USN Commc'ns, Inc.*, 2000 WL 1694325 (N.D. Ill. Oct. 20, 2000); *see also Computer Assoc. Int'l, Inc. v. Am. Fundware, Inc.*, 133 F.R.D. 166 (D. Colo. 1990) (default judgment on the issue of liability was warranted where "even assuming that maintenance of only a single, updated version of source code was, in other circumstances, a bona fide business practice, any destruction of versions of the code after service of complaint could not be excused as a bona fide business practice").

<sup>92</sup> *See, e.g., Phoenix Four, Inc. v. Strategic Res. Corp.*, 2006 WL 1409413 (S.D.N.Y. May 23, 2006) (failure to timely locate and produce information from computer server amounted to "gross negligence" warranting monetary sanctions against the defendants and their counsel).

<sup>93</sup> *See, e.g., Invision Media Commc'ns, Inc. v. Fed. Ins. Co.*, 2004 WL 396037 (S.D.N.Y. Mar. 2, 2004) (the plaintiff's discovery misconduct, including disregard of discovery obligations, misleading statements regarding the existence and location of evidence, and failure to make reasonable inquiries warranted sanctions); *Keir v. Unumprovident Corp.*, 2003 WL 21997747 (S.D.N.Y. Aug. 22, 2003) (the defendant was not sufficiently diligent in complying promptly with the court's preservation order and backup tapes were inadvertently overwritten); *Linnen v. A.H. Robins Co., Inc.*, 1999 WL 462015 (Mass. Super. Ct. June 16, 1999) (backup tapes were recycled in contravention of a court's preservation order); *GTFM, Inc. v. Wal-Mart Stores, Inc.*, 2000 WL 1693615 (S.D.N.Y. Nov. 9, 2000) (the defendant's misrepresentations about computer capabilities warranted monetary sanctions of \$109,753.81); *Crown-Life Ins. Co. v. Craig*, 995 F.2d 1376 (7th Cir. 1993) (an attorney's affidavit that all responsive documents had been produced was "blatantly false," given that the party had not produced raw data); *see also Tulip Computers Int'l B.V. v. Dell Computer Corp.*, 2002 WL 818061 (D. Del. Apr. 30, 2002).

<sup>94</sup> Non-employee sources of documents are likely to contain dynamic data—that is, electronically stored information which changes on a regular basis, such as websites or databases.

<sup>95</sup> THE SEDONA GUIDELINES, Comment 5.f.

key players are not destroyed through janitorial or other automated systems. As long as their accessible documents are not destroyed, the company should in most cases be able to continue with normal disaster recovery and recycling procedures.<sup>96</sup>

Issuing the notice may be only the first step, however, as there may be an ongoing need to follow up to ensure that the litigation hold notice is understood by the relevant individuals and is being properly observed. As the *Zubulake* court stated in its fifth opinion: “A party’s discovery obligations do not end with the implementation of a ‘litigation hold’—to the contrary, that’s only the beginning. Counsel must oversee compliance with the litigation hold, monitoring the party’s efforts to retain and produce the relevant documents.”<sup>97</sup> The court further counseled that “[t]he litigation hold instructions must be reiterated regularly and compliance must be monitored.”<sup>98</sup> Sending a quarterly or semi-annual legal hold notice reminder to the employees that reiterates the content of the legal hold notice is a good policy. If the notice was sent via email, consider attaching the original notice to the reminder.

### *Contents of a Legal Hold Notice*

The legal hold notice must properly convey the scope of material that has to be preserved, but does not necessarily have to contain a detailed list of the content of documents to be preserved. It should be tailored to the litigation at issue and give clear instructions about what needs to be preserved, describing in broad terms the subject areas of interest, and relevant time frames. The legal hold should also clarify the types of documents to be preserved, possibly including a summary of the new definition of a document under the Federal Rules of Civil Procedure. The goal is to make sure relevant documents are retained, so err on the side of being over-inclusive. The use of broad categories has the additional benefit of making the preservation notice easier to follow, as it saves the custodian from having to perform a detailed analysis to determine if a document must be preserved.

The following is a checklist of information that counsel should consider including in a legal hold:

- Indication that the communication is Attorney-Client Privileged.
- Name of the case.
- Description of the claims.
  - An accurate, but general, summary of the claims that have been, or are anticipated to be, asserted by or against the party.
  - Broad enough to describe for custodians the universe of the potentially relevant documents.
- Explicit notice that normal document retention has been suspended.
- Description of the subject matter of relevant documents.
- Description of categories of documents to preserve, including a description of what the word “document” means.
- Instruction to err on the side of preserving a document if it is questionable whether it should be preserved.
- Instruction on any affirmative steps that must be taken, other than not deleting, to preserve documents.
- Direction for handling new documents.
  - Consider whether the claims and issues relate to past conduct only, or whether they also relate to future or continuing conduct.
  - Clearly state whether there is a continuing duty to retain new documents that are created after the date of the notice and may be relevant to the subject matter of the claims.
- A prominent warning that not complying with the notice may result in the loss of relevant documents and potentially subject the company to sanctions.
- Instruction regarding what custodians should do with their documents if they change computers, transfer to a new department, or leave the company.
- Instruction regarding what custodians should do if they run out of space to store documents.
- Instruction for how to suspend any automatic janitorial programs (e.g., how to except documents from deletion, how to move documents into folder not subject to deletion).

<sup>96</sup> THE SEDONA GUIDELINES, Guideline 3, Comment 3.d. at 28.

<sup>97</sup> *Zubulake V*, 229 F.R.D. at 432.

<sup>98</sup> *Id.*

- Information about who the custodians should contact with questions.
- Contact information for the legal department.

Since legal hold notices should be sent out as soon as possible after a trigger event occurs, counsel may not yet have received a complaint or any discovery requests. Counsel should re-evaluate the legal hold notice when formal pleadings are received, but should also keep in mind that the complaint could be amended or additional requests could be served in the future.<sup>99</sup> Counsel should also make efforts to keep any revisions to the legal hold notices as consistent as possible.<sup>100</sup>

### ***Implement a Policy to Preserve Documents from Employees who Leave the Company***

If an employee is placed under legal hold, that person's documents must be maintained if s/he leaves the company. There should be a detailed policy in place that requires the human resources department to notify both the legal and information technology departments any time an employee leaves the company. Only after the names are checked against a list of legal hold notices will IT then be authorized to delete the former employee's documents in accordance with the corporate retention policy. Companies are increasingly finding it beneficial to set up databases to maintain this information and provide some level of automation with regard to notifications and related procedures.

### ***Ensuring Preservation—Collection of Documents***

The same level of thought and detail necessary to identify and preserve relevant documents should also be used in their collection. An important step is to keep a description of the guidelines and procedures followed in collecting the documents. On a technical level, make sure the party doing the collecting understands the need to maintain the integrity of the electronic data,

including maintaining the file structure of documents and email. Electronic documents are dynamic and may be easily altered.<sup>101</sup> To avoid potential claims of evidence spoliation, be aware of the ways that electronic documents may be altered. Turning on a computer system, using automatic update fields, recycling disaster recovery media, system maintenance activities, saving new data, or installing new software may all inadvertently cause documents to be altered or modified. The format in which documents are collected, as well as the step-by-step procedures used in the collection, should be included in counsel's collection guidelines.

A subtle but important aspect of document collection is to avoid, to the extent possible, disruption to the client and custodians. Again, this will require counsel to coordinate with the client's IT personnel. Counsel and the client may decide that outside counsel should collect the documents; or it may be simpler and less disruptive to have the client's IT staff, working under instruction from legal, collect the client's files. Depending on the configuration of client's computer systems, it is possible that most of the relevant electronic material may be collected remotely; *i.e.*, without physically touching the custodian's computer. If a custodian's computer must be directly accessed, it is advisable to schedule this around the custodian's schedule. Not only will this save the client lost work time, but also it lowers the risk of collection errors or omissions that may result if the collection takes place in a hurried fashion.

After documents have been collected, counsel should consider the method used to store documents. It is helpful to create an archive or library of documents that is well-organized and easily accessible. Counsel has discretion in the method they use to retain documents;<sup>102</sup> however, maintaining documents in an inaccessible format can lead to unnecessary expense when it comes time to review and produce documents.<sup>103</sup>

<sup>99</sup> THE SEDONA GUIDELINES, Comment 5.f.

<sup>100</sup> *Id.*

<sup>101</sup> Electronic documents contain hidden information, called metadata, which can easily be altered when documents are accessed. Care should be taken to keep the metadata intact. For a more comprehensive discussion of metadata, see Todd Nunn, *Uncertain and Unseen, Pending Amendments to the Federal Rules Should Provide Guidance to Handling Metadata*, Law and Technology News, January 2006.

<sup>102</sup> Zubulake IV, 220 F.R.D. at 218.

<sup>103</sup> *Quinby v. WestLB AG*, No. 04 CV 7406, 2006 WL 2597900 (S.D.N.Y. Sept. 5, 2006) (the court declined to shift costs to the plaintiff of restoring documents from backup tapes for former employees when the defendant knew they were potentially relevant to litigation at the time they were placed on backup tape).

Regardless of what decisions are made regarding the collection process, make sure to track all decisions that led to the conclusions. Keep detailed accounts of all communications with IT staff to avoid later claims of misunderstanding. Retain any document collection questionnaires or interview forms. Keep a log not only of the employees and sources from which documents were collected, but also those sources that were considered and rejected. All of these will greatly diminish the chance of later spoliation charges.

### **Preservation Issues for Parties Seeking Discovery of Electronic Documents**

Attention to preservation issues extends beyond a party's need to fulfill its own obligations. Litigation counsel should also consider what steps might be appropriate to ensure preservation of information under the control of the opposing party. The most effective approach is to consider both aspects of preservation in tandem—keeping in mind that discovery requests or other demands you make on the opposing party that have preservation implications may well be reciprocated. Be cautious in making any request or demand if your client would object or be hard-pressed to comply, were they to be presented with a similar request or demand.

#### *Address Preservation of Evidence Concerns Early*

As with one's own preservation plan, consideration of what steps are needed to ensure the preservation of information under the control of the opposing party should take place as early as possible. The earlier both parties are focused on preservation issues, the less likely crucial information will be lost. Recognizing that there is no substitute for frank discussions between the parties regarding what information is relevant, and what reasonable steps might be followed to preserve such information, the Federal Rules of Civil

Procedure now require such discussion as part of the meet and confer process.<sup>104</sup>

#### *Consider Notifying Opposing Counsel in Writing*

The first step to ensure that information under the control of the opposing party is preserved is to make sure that the opposing party is aware of the need to preserve it. As discussed earlier, the duty to preserve electronically stored materials is triggered when a party has notice that the evidence is relevant to litigation, or when a party should have known that the evidence may be relevant to future litigation. Serving the opposing party with a properly drafted complaint and discovery requests clearly should serve this purpose. But in situations where the service of either the complaint or the discovery requests is expected to be delayed, counsel may want to consider sending a preservation of evidence letter to ensure that the opponent is on notice as early as possible of the need to preserve potentially relevant documents in advance of discovery requests.<sup>105</sup>

There are several elements to include in a preservation of evidence letter, though the exact content and construction of the letter will vary depending on such factors as whether or not a complaint has been served, your familiarity with the opposing party's operations and systems, and what previous communications have taken place between the parties. The first element to include is an explanation of the existence or imminence of litigation and the nature of the litigation. If no previous communication has taken place between the parties, this aspect of the letter will likely require more attention than where, for example, the opposing party has already been served with a complaint. The letter should describe the types of evidence to be preserved, both in terms of the subject matter and in terms of the possible locations of the evidence. Where counsel has adequate knowledge of opposing party's systems and operations to do so, the letter should identify the indi-

<sup>104</sup> FED. R. CIV. P. 26(f) (stating that parties must confer “to discuss any issues relating to preserving discoverable information”).

<sup>105</sup> See, e.g., *Wiginton v. CB Richard Ellis, Inc.*, 2003 WL 22439865, at \*4 (N.D. Ill. Oct. 27, 2003) (“[T]he [preservation letter] is significant because it alerted CBRE to the types of electronic information (within the realm of all relevant documents) that were likely to be requested during discovery. Ultimately, CBRE's duty was... to preserve evidence that it had notice would likely be the subject of discovery requests. CBRE cannot now claim that it did not know that electronic data (such as e-mails or Internet use records) were likely to be the subject of discovery requests.”).

viduals, by name or by position, within the company that may possess relevant electronic evidence, and describe the material to be preserved with specificity. If the material's relevance to the litigation is not immediately apparent, a brief explanation of its relevance may be warranted. Finally, ask that the evidence be located immediately and preserved.

Preservation of evidence letters serve a limited but useful function. Preservation of evidence letters can reduce the risk that the opposing party will destroy relevant documents. If drafted properly, the preservation letter provides a party with clear notice that it may have relevant evidence, and can also be useful in helping them identify and preserve the likely sources of that evidence. Keep in mind, however, that a preservation of evidence letter by itself does not create a duty to preserve every shred of information described in the letter. In fact, courts may cast an unsympathetic eye on a preservation of evidence letter that is overly broad and seems

designed with an eye toward establishing a foundation for spoliation, rather than an honest effort to alert the opposing party of the need to preserve evidence.<sup>106</sup>

### *If Circumstances Warrant, Obtain a Preservation Order from the Court*

So long as both parties are acting in good faith, most preservation issues can be resolved without the direct involvement of the court.<sup>107</sup> There may, however, be times where a party acts in bad faith. Where willful destruction of evidence is a real risk, be prepared to take action beyond notifying opposing counsel in writing of the duty to preserve potentially responsive documents. If there is good cause to believe a litigant or third party is apt to alter or destroy relevant electronic evidence, consider obtaining an order to preserve evidence,<sup>108</sup> or an order permitting the seizure of computers and storage media.<sup>109</sup>

Courts will consider a number of factors in decid-

<sup>106</sup> See, e.g., *Frey v. Gainey Transp. Servs., Inc.*, 2006 WL 2443787 (N.D. Ga. Aug. 22, 2006) (Questioning the plaintiff's counsel's 15-page "spoliation letter," the court observed: "Such an extensive request for materials certainly would lend itself to an effort on any plaintiff's part to sandbag a defendant in the event that any of those materials were not preserved.... [I]t is difficult to allow a potential plaintiff to make an end run around the Federal Rules of Civil Procedure by filing a preemptive 'spoliation' letter.").

<sup>107</sup> See, e.g., FED R. CIV. P. 26(f), advisory committee's note ("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.")

<sup>108</sup> *Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668 (D. Kan. Mar. 24, 2006) (during initial case management conferences, the court ordered mirror imaging of all of the defendants' computers and peripheral equipment to be done at the plaintiffs' expense, and ordered the parties to meet and confer on appropriate search protocol that would address the issue of protection of attorney client privilege and non-business related personal information); see also *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645 (D. Minn. 2002) (the plaintiff's motion for expedited discovery, entry of a preservation order and to appoint neutral computer forensics expert to take mirror image of the defendants' hard drives was granted, even though no discovery had yet been propounded); *Hypro, LLC v. Reser*, 2004 WL 2905321 (D. Minn. Dec. 10, 2004) (in light of the defendant's previous attempt to delete incriminating email and documents from his company laptop, the court entered an order requiring all parties to preserve and protect evidence); *ProPath Servs., L.L.P. v. Ameripath, Inc.*, 2004 WL 2389214 (N.D. Tex. Oct. 21, 2004) (the court entered a preliminary injunction prohibiting the defendants from, among other things, deleting, destroying, or altering any document, email, or computer drive containing any ProPath or ProPath related information, and required the defendants to segregate said items into a confidential file not to be used in their business); *Kadant v. Seeley Mach., Inc.*, 244 F. Supp. 2d 19 (N.D.N.Y. 2003) (the plaintiff's motion for preliminary injunction was granted; the defendants were enjoined from destroying, erasing, or altering any of its computer-stored information that concerned any of the plaintiff's claims against them).

<sup>109</sup> *Henry v. IAC/Interactive Group*, 2006 WL 354971 (W.D. Wash. Feb. 14, 2006) (granting a preliminary injunction forcing the plaintiff to return computers and electronic files to the defendants after a forensic firm first removed the plaintiff's own privileged documents at her expense); *AutoNation, Inc. v. Hatfield*, 2006 WL 60547 (Fla. Cir. Ct. Jan. 4, 2006) (granting temporary injunctive relief and ordering a forensic inspection of a personal computer); *QZO, Inc. v. Moyer*, 594 S.E.2d 541 (S.C. Ct. App. 2004) (the trial court entered a TRO on the same day a complaint was filed,

ing whether to enter a preservation order. For example, a Pennsylvania court set forth a three-part balancing test for evaluating a motion for a preservation order: (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 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 physical, spatial, and financial burdens created by ordering evidence preservation.<sup>110</sup> When seeking a preservation order, be sure to address these considerations in the motion.

In extreme cases where a risk of destruction is particularly high, *i.e.*, where the facts demonstrate that the adverse party has the opportunity to conceal or destroy evidence, and that the party is likely to take the opportunity for deceptive conduct, *ex parte* relief may be possible.<sup>111</sup>

### ***If Relevant Evidence Is Destroyed, Consult a Computer Forensics Expert and Consider Seeking Appropriate Sanctions***

Despite the precautions counsel takes, counsel may discover that relevant evidence has been altered or deleted, either innocently or maliciously. Where the altered or deleted files are likely to contain information that is particularly relevant, counsel may need to consult with a computer forensics expert to recover the missing evidence.

### ***Review Material Produced and Follow Up Promptly***

Once the opposition has provided responses and documents to the discovery requests, be diligent in reviewing it, and follow up if there appear to be discrepancies. For example, confirm that the universe of ESI produced covers the relevant time period, and that there are no large gaps of time for which no information has been produced.<sup>112</sup> Similarly, determine whether email has been produced for all the key players. In some situations, it may be useful to

---

ordering the defendant to surrender immediately a computer belonging the parties' former partnership); Dodge, Warren & Peters Ins. Servs., Inc. v. Riley, 130 Cal. Rptr. 2d 385 (Ct. App. 2003) (preliminary injunction requiring preservation of electronic evidence upheld; the defendants were prohibited from destroying any electronic storage media and required to allow a court-appointed expert to copy all of it, to recover lost or deleted files, and to perform automated searches of evidence under guidelines agreed to by parties or set by court); Gates Rubber Co. v. Bando Chem. Indus., Ltd., 167 F.R.D. 90 (D. Colo. 1996) (court allowed expedited discovery and issued a site inspection order, allowing the plaintiff to enter the defendant's premises to locate and copy materials, including electronic records, for preservation); Ranta v. Ranta, 2004 WL 504588 (Conn. Super. Ct. Feb. 25, 2004) (the plaintiff wife was ordered to stop using the couple's laptop computer and deposit it with the clerk of court); Physicians Interactive v. Lathian Sys., Inc., 2003 WL 23018270 (E.D. Va. Dec. 5, 2003) (court granted limited expedited discovery to enter the defendant's premises and obtain a "mirror image" of the computer equipment containing electronic data relating to the defendants' alleged attacks on the plaintiff's server; discovery limited to information on the defendants' computers related to the alleged attacks, and assistance of computer forensic expert required).

<sup>110</sup> Capricorn Power Co., Inc. v. Siemens Westinghouse Power Corp., 220 F.R.D. 429 (W.D. Pa. 2004).

<sup>111</sup> Comcast of Ill. X, LLC v. Till, 293 F. Supp. 2d 936 (E.D. Wis. 2003) (court granted the plaintiff's *ex parte* motion for expedited discovery and for a preservation order); Carlton Group, Ltd. v. Tobin, 2003 WL 21782650, at \*8 n.8 (S.D.N.Y. July 31, 2003) (court granted an *ex parte* application for TRO and related relief in order to locate and recover stolen information, and ordered return of laptops and "bit stream copying" of the defendants' computers to preserve deleted data). *But see* Harrison v. Jones, Walker, Waechter, Poitevent, Carrere & Denegre, L.L.P., 2004 WL 2984815 (E.D. La. Dec. 9, 2004) (participation by former employer and its attorneys in the execution of state court's preservation order authorizing imaging of the plaintiffs' hard drives may support state law claims of trespass, invasion of privacy, and abuse of rights); First Techn. Safety Sys., Inc. v. Depinet, 11 F.3d 641 (6th Cir. 1993) (*ex parte* order permitting the plaintiff and its counsel, with U.S. Marshal, to enter the defendants' business premises and inventory and impound computer records and copy and inventory business records was abuse of discretion).

<sup>112</sup> *See, e.g.*, Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99 (2d Cir. 2002) (email from relevant time period missing).

compare the productions received from different parties or third parties for any major discrepancies, as emails sent between them ought to be produced by each of them.<sup>113</sup> Where there are reasonable grounds to believe that the opposition has not complied with its discovery obligations, promptly follow up with the party—or the court, as necessary. The appropriate level of follow up will depend on the severity of the discovery failing, as well as the opposing party's promptness and cooperation in remedying it. In extreme cases, where for example there is evidence that relevant information has been willfully destroyed

or withheld, you may consider seeking direct access to its computer systems.<sup>114</sup>

### *Employ Other Discovery Tools*

A number of other discovery tools are available to parties engaging in electronic discovery to ensure that preservation obligations are being met. If the litigation is in federal court, it is likely that the other side will disclose the identities and locations of key players and documents in its Rule 26(a)(1) disclosures. In addition, interrogatories may be useful to obtain basic information about a party's computer systems

<sup>113</sup> See, e.g., *Cumis Ins. Co. v. Diebold, Inc.*, 2004 WL 1126173 (E.D. Pa. May 20, 2004) (the plaintiff convinced the court that the defendant may not have satisfied its discovery obligations by showing that responsive Diebold documents and emails had been obtained from other sources, but had yet to be produced by Diebold itself).

<sup>114</sup> See, e.g., *Alexander v. F.B.I.*, 186 F.R.D. 78 (D.D.C. 1998) (examination of a former official's hard drive and servers allowed in order to determine whether responsive documents that were not produced actually existed); *Ukiah Auto. Invs. v. Mitsubishi Motors of N. Am., Inc.*, 2006 WL 1348562 (N.D. Cal. May 17, 2006) (where the defendant asserted that many financial records were missing from the plaintiff's paper production, the magistrate ruled that, unless the plaintiff was able to produce the relevant documents in electronic form on its own, the plaintiff would be required to produce its computer to an agreed-upon neutral inspector within 30 days and shoulder the cost of such inspection); *Tilberg v. Next Mgmt. Co.*, 2005 WL 2759860 (S.D.N.Y. Oct. 24, 2005) (allowing a forensic search of the defendant's computer system and additional discovery by the plaintiff after the discovery cut-off where a partial forensic search showed that relevant documents existed on the defendant's email servers, central server, and individual work-stations, and where the plaintiff presented relevant documents received from third parties which were never produced by the defendant); *GTFM, Inc. v. Wal-Mart Stores, Inc.*, 2000 WL 335558 (S.D.N.Y. Mar. 30, 2000) and 2000 WL 1693615 (S.D.N.Y. Nov. 9, 2000) (the plaintiffs' motion for on-site inspection of computer records granted); *Renda Marine, Inc. v. U.S.*, 58 Fed. Cl. 57 (2003) (in view of a key player's practice of deleting relevant e-mail documents, which continued even after the lawsuit commenced, the court ordered the defendant to provide access to the defendant's hard drive). *But see Floeter v. City of Orlando*, 2006 WL 1000306 (M.D. Fla. Apr. 14, 2006) (denying the plaintiff's motion to gain entry into the Orlando Police Department offices to inspect its computer hard drives since the hard drives contained much irrelevant information and could contain information about ongoing criminal investigations, confidential sources, and the like, and the plaintiff had not made any showing that he had requested information contained on the computer hard drives which the city had failed to produce); *Williams v. Mass. Mut. Life Ins. Co.*, 226 F.R.D. 144 (D. Mass. 2005) (court denied the plaintiff's request for a forensic search of a former employer's information systems where the plaintiff offered no credible evidence that the defendants were unwilling to produce computer-generated documents or that the defendants had withheld relevant information); *Menke v. Broward County Sch. Bd.*, 916 So. 2d 8 (Fla. Dist. Ct. App. 2005) (quashing administrative law judge's order allowing a school board's expert unfettered access to a teacher's home computers to discover whether they contained various categories of information; there was no evidence of any destruction of evidence or thwarting of discovery, and an order afforded no protection against the disclosure of confidential or privileged information); *Bethea v. Comcast*, 218 F.R.D. 328 (D.D.C. 2003) (court denied the plaintiff's motion for an order compelling the defendants to allow her to enter upon their premises, inspect their computer systems and related programs, and copy any relevant information, since the plaintiff was merely speculating that the defendants failed to satisfy their discovery obligations); *In re Ford Motor Co.*, 345 F.3d 1315 (11th Cir. 2003) (a discovery order granting the plaintiff unlimited and direct access to Ford's databases was an abuse of discretion in the absence of a factual finding of some non-compliance with discovery rules by Ford); *McCurdy Group, LLC v. Am. Biomedical Group, Inc.*, 2001 WL 536974 (10th Cir. May 21, 2001) (the defendant's skepticism that the plaintiff had not produced copies of all responsive documents did not entitle the defendant to conduct a physical inspection

and records retention policies.<sup>115</sup> Counsel may also take Rule 30(b)(6) depositions to uncover important information about electronic evidence controlled by the opponent. Depositions taken early in the case may

provide the information needed to craft document requests, while depositions later on may provide a means to test compliance with discovery obligations.

---

of the plaintiff's hard drives); *Convolve, Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162 (S.D.N.Y. 2004) (the court rejected the plaintiff's request for direct access to Compaq's hard drives, servers, and databases since the plaintiff failed to show widespread destruction or withholding of relevant information by Compaq).

<sup>115</sup> *Treppel v. Biovail Corp.*, 233 F.R.D. 363 (S.D.N.Y. 2006) (the defendants were ordered to treat a Document Retention Questionnaire and the plaintiff's supplemental letter inquiries regarding electronic document maintenance and retention as interrogatories and provide substantive responses); *Sonnino v. Univ. of Kansas Hosp. Auth.*, 220 F.R.D. 633 (D. Kan. 2004) (the defendant was ordered to provide a complete and full response to interrogatories seeking information about computer and email systems since the defendant's "very brief and general response" was insufficient); *see also* *Concerned Citizens of Belle Haven v. Belle Haven Club*, 223 F.R.D. 39 (D. Conn. 2004) (the court granted the plaintiff's motion to compel the defendants to respond to interrogatories and requests for admissions relating to the database compiled by the plaintiffs).

