WHITE PAPER

E-Mail Discovery
Worst Case Scenarios vs. Best Practices

Jeffrey Plotkin
Attorney at Law
Eiseman Levine Lehrhaupt
& Kakoyiannis, P.C.
845 Third Avenue
New York, NY 10022

Compliments of

now from

TABLE OF CONTENTS

ABOUT THE AUTHOR

Jeffrey Plotkin is a Partner in the Litigation Department of the New York City law firm of Eiseman, Levine, Lehrhaupt & Kakoyiannis, P.C. He formerly served as Assistant Regional Administrator of the Securities and Exchange Commission's New York Regional Office, in the Division of Broker-Dealer Enforcement.

Mr. Plotkin is a consultant for KVS, Inc., a leading provider of e-mail archiving and management software. He has authored other White Papers respecting legal issues surrounding e-mail, including "Coping with Broker-Dealer Regulations Concerning E-Mail," and "Corporate Governance – The Impact on Your IT Department," both available through www.kvsinc.com. *Mr. Plotkin has been quoted in the Wall Street Journal, Investment News, and Wall Street & Technology, with respect to regulatory issues involving e-mail.*

For further information concerning Mr. Plotkin, please visit www.SECDefense.com.

INTRODUCTION

This White Paper addresses the complications that regularly arise during discovery in civil litigation as a result of a corporate defendant's faulty or insufficient systems and procedures for e-mail retention and management. These complications, all of which are avoidable, increase litigation costs so exponentially that, in many cases, settlement becomes the only viable option.

The e-mail discovery issues addressed herein fall into two broad categories. The first category concerns "cost-shifting," particularly: (1) which party should pay the extraordinary costs associated with retrieval of e-mails from disaster recovery backup tapes; and (2) which party should pay the substantial costs associated with hard drive discovery for (a) e-mails stored in a decentralized, non-network environment (*e.g.*, where responsive e-mails are dispersed among the hard drives of individual users); and (b) e-mails that have been "deleted" from mailboxes and now reside as on the hard drive as "residual" data?

The second category concerns retention of e-mails, particularly: (1) what duty does a party generally have to preserve e-mails prior to and during litigation; and (2) what sanctions are appropriate against a party who fails in that duty?

I.

WHO PAYS FOR E-MAIL DISCOVERY?

A. Disaster Recovery

1. Backup Tapes

Historically, as a disaster recovery mechanism, companies have utilized commercially available software to take a periodic "snapshot" of the data on the company's servers, including e-mail files. That data is stored on magnetic tape, which is commercially available

in various formats. Vast amounts of data can be stored on a single magnetic tape. If a catastrophic event occurs, the data previously captured on magnetic tape from the last backup period can be reloaded to allow the company's computer systems to startup again with minimal loss.

> Back-up tapes . . . are not archives from which documents may easily be retrieved. The data on a backup tape are not organized for retrieval of individual documents or files, but for wholesale, emergency uploading onto a computer system. There, the organization of the data mirrors the computer's structure, not the human records management structure if there is one.

Rowe Entertainment, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421 (S.D.N.Y. 2002) (citation omitted).

Companies utilize different disaster backup protocols. A typical backup protocol provides for creation of back up tapes at three intervals: end of each business day; end of each business week; and end of each business month.[1] Nightly backup tapes may be kept until the end of the week or month, weekly tapes may be kept until the end of the month or year, and monthly tapes may be kept until the end of the year or for a number of years. After the expiration of the retention period for each backup tape, the tapes are recycled and overwritten.

Periodic backups necessarily entail the loss of certain e-mail. If employees delete e-mails from the server prior to the expiration of a given backup period, that e-mail would not appear in the following periodic snapshot of the e-mail files. For instance, if an employee deleted an entry from his e-mail box prior to the end of the month, that entry would not be captured on the monthly back-up tapes (but might appear on the daily or weekly backup tapes, if they still exist). On the other hand, unless a user deletes e-mails between backups, each

[1] *See, e.g., Wiginton v. Ellis*, 2003 WL 22439865 at *2 (N.D. Ill. Oct. 27, 2003). Some companies also employ incremental backups, *i.e.*, a backup of files that have changed since the last backup.

backup tape may contain duplicate e-mails, *i.e.,* e-mails that were captured on previous backup tapes.

It is a sound business practice to utilize magnetic backup tapes as a disaster recovery mechanism. However, litigation complications arise when the backup tapes are the only place where an opposing party can discover relevant e-mails.[2] In order to access e-mail on a disaster recovery backup tape, the data has to be "restored."

Restoration of e-mails from backup tapes is a lengthy and expensive process. Among other things, the company must first locate and catalog the tapes that may contain the relevant mailbox files. During the restoration process, the company must clean and check the functionality of the tape drive regularly, because backup tapes physically get dirty or dusty from years of storage.[3] Once the data is accessed,[4] the company must determine which directories on the backup tape need to be restored. The company then must clear sufficient disk space on a hard drive, because each backup tape represents a snapshot of the server's hard drive on a given date, and each date must be restored separately on to a hard drive.[5] The company then restores the responsive data onto a hard drive.

---

[2] A company's duty to preserve backup tapes, once it has notice of a potential or actual litigation, is discussed in Section II below.

[3] Successful restoration of back-up tapes cannot be guaranteed in any individual instance, because the tapes may have been corrupted during storage (*e.g.*, moisture corruption). And the attempts to restore the back-up tapes may corrupt them even further.

[4] Because of advances in technology, a company may no longer currently utilize the tape format that it utilized to backup the data years before. As a result, the company may no longer have the hardware necessary to access and utilize a particular tape format, or it may no longer maintain the software it previously utilized to create the backup.

[5] In *Concord Boat Corp. v. Brunswick Corp.*, 1997 WL 33352759 at *8 – 9 (E.D. Ark. Aug. 29, 1997), defendant's information systems support manager informed the court that "restoring a backup copy of the . . . e-mail system onto . . . [the] Host Server would destroy the current version of the . . . e-mail system and jeopardize [the company's] continuing data processing activities. It would therefore be necessary to duplicate [the company's] computing environment as it existed at the time the back up tape was created on a separate computer system."

Once restoration of the data is accomplished, commercially available software could be used to extract a particular individual's e-mail file. For instance, the e-mail file can be exported onto a Microsoft Outlook data file, which in turn can be opened in Microsoft Outlook, a common e-mail viewer application. A user could then browse through the mail file and sort the mail by recipient, date or subject, or search for key words in the body of the e-mail. Also, software may be used to "de-duplicate" the e-mail files, *i.e.*, remove duplicate copies of e-mails.

Complications regularly arise during the restoration process. E-mail attachments in formats that cannot be searched electronically, such as pdf. files (scanned image files), must be converted into text-searchable files.[6] Further, the passwords for protected e-mails and attachment files must be "broken." And in many instances where the e-mail files cannot be exported successfully to commercially available software, companies must develop a software script to run the requested search phrases through the restored data.

The estimated and actual costs for restoring backup tapes and searching restored e-mails vary widely, depending on whom you talk to. However, in most large cases, the costs are extraordinary. *See Medtronic Sofamore Danek, Inc. v. Michelson*, 2003 WL 21468573 at * 11 (W.D. Tenn. May 13, 2003) (consultant charged a total of $605,000 to restore, search, and de-duplicate 124 sample backup tapes, or $4,881 per tape); *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280, 282-83 (S.D.N.Y. 2003) (consultant charged an average of $2,304.92 per backup tape to restore and text-search e-mails).

[6] Where a company wishes to print-out hard copies of all restored e-mails and attachments, and search the documents manually rather than electronically for responsiveness and privilege, ease of mass printout may be facilitated by converting all e-mails and attachments to a TIFF (Tagged Image File Format). *See, e.g., Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, 2002 WL 246439 at *2 (E.D. La. Feb. 19, 2002).

2. "Cost-Shifting" of Backup Tape Restoration and Search

Historically, the party responding to a discovery request bears the costs of producing responsive and relevant materials in its possession, custody, and control. However, the responding party "may invoke the district court's discretion under [Federal Civil Procedure] Rule 26(c)[7] to grant orders protecting him from 'undue burden or expense' in doing so, including orders conditioning discovery on the requesting party's payment of the costs of discovery." *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 358, 98 S. Ct. 2380, 2393 (1978).

In the past, in the realm of paper-based discovery, it was the rare case where a defendant requested that the court shift the costs of discovery to the plaintiff, and the even rarer care where the court granted such request. However, in the current realm of electronic discovery, defendants increasingly are asking the courts to shift some or all of the costs of electronic discovery, particularly backup tape restoration, to the requesting party.

The courts are mindful that their ultimate decision on this issue may represent the defining moment in the litigation. As one court noted:

> If the likelihood of finding something was the only criterion, there is a risk that someone will have to spend hundreds of thousands of dollars to produce a single e-mail. That is an awfully expensive needle to justify searching a haystack. It must be recalled that ordering the producing party to restore backup tapes upon a showing of likelihood that they will contain relevant information in every case gives the plaintiff a gigantic club with which to beat his opponent into settlement. No corporate president in her right mind would fail to settle a lawsuit for $100,000 if the restoration of backup tapes would cost $300,000. While that scenario might warm the cockles of certain lawyers' hearts, no one would accuse it of being just.

McPeek v. Ashcroft, 202 F.R.D. 31, 34 (D.D.C. 2001).

---

[7] Pursuant to FRCP 26(c), a court may enter "any order which justice requires to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including . . . (2) that the . . . discovery may be had only on specified terms and conditions . . . .". The civil procedure rules of the various states have similar provisions.

An instructive case that will be discussed at length here is *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) ("*Zubulake I*"), not only because it articulates a currently accepted standard for cost-shifting in backup tape cases, but also because it minutely details the aggravations, burdens and costs attendant to producing e-mails from backup tapes.

UBS, a broker-dealer registered with the SEC, backed up its e-mails in two ways, on magnetic backup tapes or on optical disks.[8] In response to Zubulake's broad e-mail discovery request, UBS preliminarily determined that responsive e-mail files were contained on a total of 94 backup tapes. Before UBS undertook the task of restoring and searching the backup tapes for responsive e-mails, it petitioned the court to shift the cost of production to Zubulake to protect it from undue burden or expense, pursuant to FRCP 26(c).

The *Zubulake* court stated that it first had to ascertain whether the data was kept in an "accessible" or "inaccessible" format in order to determine whether production of electronic data was unduly burdensome or expensive under FRCP 26(c). The court listed five categories of electronic data, from most accessible to least accessible -- the second least accessible being "backup tapes."

The court stated:

> The disadvantage of tape drives is that they are sequential-access devices, which means that to read any particular block of data, you need to read all the preceding blocks. As a result, the data on a backup tape are not organized for retrieval of individual documents or files because the organization of the data mirrors the computer's structure, not the human records management structure. Backup tapes also typically employ some sort of data compression, permitting more data to be stored on each tape, but also making restoration more time-consuming and expensive, especially given the lack of uniform standard governing data compression.

Id. at 319 (quotations marks, brackets, ellipses, footnotes and citations omitted).

[8] In particular, UBS stored on optical disk outgoing and incoming external e-mail to and from registered traders. Internal e-mails, however, were not stored on this system. Because the optical disks were easily searchable using publicly available software, the court ordered UBS to search all optical disks at its cost.

Because it found that the UBS backup tapes were "inaccessible," the court ruled it was appropriate to consider cost-shifting. Using as it starting point a "balancing approach" articulated by courts in other e-discovery disputes (primarily the eight-factor test articulated by *Rowe*), the court fashioned a cost-shifting test with seven factors, in the following descending order of importance:

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

Id. at 321-22.

Given the uncertainty of whether the backup tapes would yield probative evidence, the court ordered UBS, at its own cost, to restore and produce responsive e-mails from a sample of five backup tapes selected by Zubulake. The court ordered that UBS submit an affidavit detailing the results of its search of the five sample backup tapes, as well as the time and money spent on the search. After further review, the court would issue a final ruling on the cost-shifting issue, based on the tangible evidence the tapes offered, and the tangible evidence of the time and cost required to restore the backup tapes.[9] *See Id.* at 323-24.

[9] This protocol (*i.e.*, initial sampling results followed by a final decision on cost-shifting) has been utilized in numerous other backup tape cases. *See, e.g., McPeek,* 202 F.R.D. at 34-35; *Linnen v. A.H. Robbins Co., Inc*., 1999 WL 462015 at *6 (Mass. Super. June 16, 1999).

Pursuant to the court's order, UBS restored and produced e-mails from the five backup tapes. *See Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003) ("*Zubulake II*"). After reviewing the results, Zubulake moved for an order compelling UBS to produce all remaining e-mails at its expense. UBS, which had revised the number of remaining backup tapes to be seventy-seven, continued to argue that the costs should be shifted entirely to Zubulake.

UBS reported to the court that it used an outside vendor to perform the restoration of the backup tapes. The consultant restored each of the tapes, yielding a total of 6,203 unique (non-duplicated) e-mails. The consultant then performed a search for e-mails containing relevant text or header terms (such as "Zubulake"), and found 1,541 responsive e-mails. UBS deemed 600 of the e-mails to be relevant and produced them.

The consultant billed UBS a total of $11,524.63 ($2,304.92 per tape). In addition, UBS incurred $4,633 in attorney fees for the document review, and $2,845 in paralegal fees for tasks related to document production. UBS also paid $432.60 in photocopying costs (reimbursed by Zubulake). The total cost of restoration and production from the five backup tapes was $19,003.43 -- almost four thousand dollars per tape. *See Id.* at 283.

UBS asked the court to shift the cost of further production, estimated to be $273,649 ($165,954 to restore and search the tapes, and $107,694 for attorney and paralegal review costs), to Zubulake.

Upon review of the search results from the five backup tapes, the court found that 68 of the 600 e-mails presented by Zubulake to the court were relevant to the case. After applying the seven part test to the facts and circumstances of the case, the court ordered that UBS bear 75% of the estimated $165,000 cost of restoring and searching the remaining

backup tapes, and 100% of the estimated $107,000 cost of reviewing and producing the electronic data once it has been converted to an accessible form. In other words, the court ordered UBS to incur an additional $240,000 to restore and search the remaining e-mails. This number, of course, did not include the legal fees and costs incurred in litigating the issue twice before the court. *See Id.* at 284-91.

Other defendants in other cases have fared better or worse in shifting some of the costs of backup tape restoration to the plaintiffs. In *Medtronic*, the court ordered defendant to bear 60% of the total estimated cost of $605,300 to restore, search, and de-duplicate e-mails from 124 sample backup tapes. That cost excluded attorney privilege review, and production costs. *See Medtronic,* 2003 WL 21468673 at *11.

In *Byers v. Illinois State Police*, 2002 WL 1264004 (N.D. Ill. June 3, 2002), even through the court found it highly unlikely that a search of backup tapes would yield relevant e-mails, the court ordered the defendant to bear 100% of the expense of restoring and searching daily backup tapes for an eight year period. However, because the defendant recently had converted to a new e-mail program that could not read the e-mails contained on the backup tapes, the court shifted the costs to plaintiff to license the old e-mail program at a cost of $8,000 month.

Because of cases like *Zubulake*, a move is afoot to amend the Federal Rules of Civil Procedure to codify cost-shifting standards in e-discovery cases. The Civil Rules Advisory Committee of the U.S. Judicial Conference currently is considering whether to propose amendments to F.R.C.P. Rule 26 addressing electronically stored data. The Committee's most-current draft of a proposed Rule 26(h)(2), with its variable alternatives, shows the inherent difficulties of framing an ironclad rule regarding cost-shifting:

> **Inaccessible electronically-stored data**. In responding to discovery requests, a party need not include electronically-stored data [from systems] created only for disaster-recovery purposes, [providing that the party preserves a single day's full set of such backup data,] or electronically-stored data that are (not [reasonably] accessible without undue burden or expense) [accessible only if restored or migrated to accessible media and format] (not accessible [reasonably available] in the usual course of the responding party's (business) [activities]). For good cause, the court may order a party to produce inaccessible electronically-stored data subject to the limitations or Rule 26(b)(2)(B), [and may require the requesting part to bear some of all of the reasonable costs of (any extraordinary efforts necessary in) obtaining such information.

Rick Marcus, *Memorandum to Advisory Committee on Civil Rules re: E-discovery rule discussion proposals* at 19-20 (Sept. 15, 2003).

3. Avoiding the Backup Tape Dilemma

UBS's dilemma in *Zubulake* was easily avoidable. UBS should have archived all its e-mails on accessible and easily searchable storage media, separately from, and in addition to, its disaster recovery backup tapes. UBS, through commercially available software, easily could have automatically journaled all its employees' e-mails to a central data store, from which archived copies of the e-mails could be created on optical disk, CD-ROM, or optical tape.[10]

Indeed, UBS, an SEC registered broker-dealer, was required to archive all its e-mails for three years in a non-erasable, non-alterable format, as proscribed by SEC Exchange Act

[10] *Accord The Sedona Principles -- Best Practices Recommendation & Principles for Addressing Electronic Document Production* at 23 (The Sedona Conference, March 2003) ("Organizations seeking to preserve data for business purposes or litigation should, if possible, employ means other than disaster recovery backup tapes. Alternatives include utilizing copies of relevant files, "snap" server copies, and targeted archive tape creation.").

Rule 17a-4(f).[11] If UBS simply had followed that rule, and had stored e-mails correctly, it would have saved hundreds of thousands of dollars of discovery costs and legal fees.

B. Hard Drive Discovery

1. Decentralized E-Mail

Another e-discovery issue that regularly arises is where the company's e-mail is not centrally stored and managed on the firm's network server. For instance, it is often the case that the only copies of responsive e-mails are located on the individual hard drives of multiple employees' personal computers or laptops. Discovery under these circumstances can get especially complicated where the individual employees' computers use a variety of different e-mail programs, so that all files cannot be reviewed by a single search program.[12]

During litigation, some companies with decentralized e-mail storage issues have attempted to shift the costs of e-discovery to the other party, with mixed results. In *Medtronic*, the court refused to shift costs, and ordered the defendant, at its own cost, to search through 300 gigabytes of individual user e-mails, using Boolean search terms provided by plaintiff's counsel. *See Medtronic*, 2003 WL 21468573 at *9.

---

[11] *See generally*, Jeffrey Plotkin, *Broker-Dealer Regulations Concerning E-Mail*, New York Law Journal, December 4, 2002. At the time the SEC's rule was promulgated, the industry standard for non-alterable, non-erasable electronic storage media was "WORM" ("write once, read many") storage on optical disk, optical tape, and CD-ROM. With WORM, digital information is permanently "burned" onto the hardware, and consequently, the information could not easily be altered or deleted. In May 2003, the SEC issued a release allowing broker-dealers to employ electronic storage systems that prevent records from being rewritten or erased without relying solely on the system's hardware features. See SEC Release No. 34-47806 (May 12, 2003). In particular, the SEC approved the use of a new storage technology that utilizes integrated hardware and software codes intrinsic to the system to prevent overwriting, erasure, or alteration of digitally stored records. The system stores an expiry or retention period with each record or file system. The system described in the SEC release is EMC's Centera. According to EMC, compared to standard WORM storage, Centera users can expect a reduction in their overall storage capacity requirement by 50%.

[12] In order to conduct a decentralized search of individual user's hard drives, a company may hire a consultant to obtain a "mirror image" of the hard drives containing e-mails, and formulate and implement a search procedure. *See Rowe*, 205 F.R.D. at 433.

In *In re Amsted Industries, Inc. "ERISA" Litigation*, 2002 WL 31844956 (N.D. Ill. Dec. 18, 2002), defendants chose not to conduct an actual hard drive search of individual user e-mails, but instead "investigated" whether responsive e-mails existed by "questioning individuals regarding e-mails on their computers." The plaintiffs argued that this investigation was inadequate and that the defendants were required to actually search the hard drive of each individual defendant and each person having access to relevant information to determine whether there is discoverable material.

The court agreed, and ruled that defendants "should also search the in-box, saved, and sent folders of any relevant individual's e-mail in the same manner. We recognize that Amsted's retention policy and its lack of a comprehensive e-mail system . . . make it unlikely that the additional searches are going to turn up relevant discovery. On the other hand, [the requested search is not] so burdensome or expensive as to require a limiting of the requests." *Id.* at *2.

2. "Deleted" E-Mails

Many e-mail users still linger under the impression that once they delete an e-mail from their mailbox, it is gone forever. This simply is not the case.

> "Deleting" a file does not actually erase that data form the computer's storage devices. Rather, it simply finds the data's entry in the disk directory and changes it to a "not used" status – thus permitting the computer to write over the "deleted" data. Until the computer writes over the "deleted" data, however, it may be recovered by searching the disk itself rather than the disk's directory. Accordingly, many files are recoverable long after they have been deleted – even if neither the computer use nor the computer itself is aware of their existence. Such data is referred to as "residual data."

Zubulake, 217 F.R.D. at 313 n. 19, *quoting* Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. Rev. 327, 337 (2000) (footnotes omitted). [13]

Under normal circumstances, a party responding to an e-mail discovery request has no obligation to attempt to restore e-mails deleted in the ordinary course of business.[14] However, plaintiffs routinely demand that corporate defendants allow them to inspect the defendants' computer systems to discover deleted e-mails that may still exist on hard drives. The courts have been amenable to ordering such discovery (including inspection not only of the company's network servers, but also of individual employees' personal computers and laptops), usually at the plaintiff's cost, where there is evidence that responsive e-mails may have been deleted.

> Aside from the occasional practice of "dumpster diving," the discovery of deleted computer documents does not have a close analogy in conventional, paper-based discovery. Just as a party would not be required to sort through its trash to resurrect discarded paper documents, so it should not be obligated to pay the cost of retrieving deleted e-mails. Thus, since there has been no showing that the defendants access . . . their deleted e-mails in the normal course of business, this factor[] tips in favor of shifting the costs of discovery to the plaintiffs.

Rowe, 205 F.R.D. at 431 (quotations marks, citation and footnote deleted).

A standard protocol has emerged from the courts in cases where the plaintiff demands inspection of the defendant's computers to search for deleted e-mails. A computer expert,

---

[13] "Deleted data may also exist because it was backed up before it was deleted. Thus, it may reside on backup tapes or similar data." *Id.*

[14] *But compare* ABA Litigation Task Force on Electronic Discovery, Standard 29(a)(iii) (Aug. 1999) ("Unless a requesting party can demonstrate a substantial need for it, a party does not ordinarily have a duty to take steps to try to restore electronic information that has been deleted or discarded in the regular course of business but may not have been completely erased from computer memory"), *with* ABA Litigation Task Force on Electronic Discovery, November 2003 Draft Amendments to Electronic Discovery Standards, Standard 29(a)(iii) (Nov. 17, 2003)("Electronic data as to which a duty to preserve may exist include data that have been deleted but can be restored"), *both available at* http://www.fjc.gov/public/pdf.nsf/lookup/ElecDi12.pdf/$file/ElecDi12.pdf

either selected by the plaintiff or acceptable to both parties, is appointed by the court to create a "mirror image" of the hard drive. The plaintiff pays the expert's fees and expenses, and the defendant makes its computers and its technical personnel available to the computer expert. After the expert completes his technical tasks, he provides to the defendant's counsel all recovered e-mails (or in some cases, provides the data to plaintiff's counsel for "attorneys'-eyes-only" review). Defendant's counsel then reviews the records for privilege and responsiveness, at defendant's expense, and makes production to plaintiff.[15]

Even though the courts typically order the plaintiffs to shoulder the costs of the expert inspection and search for deleted e-mails files, the inspection process itself creates disruption of and interference with defendant's business. Additionally, if the plaintiff does not voluntarily agree to pay the costs associated with deleted e-mail restoration, defendants must then expend significant legal fees in motion practice to resist plaintiff's attempts to impose the costs of e-mail restoration on the defendant.

And finally, as discussed at length in Section II below, if a plaintiff learns through a hard drive inspection of the computer's computers that the company's employees have deleted responsive e-mails from hard drives in violation of an obligation to preserve relevant evidence, such plaintiff will seek, and may well obtain, significant sanctions against the company for "spoliating" evidence.

3. Avoiding Hard Drive Discovery Problems

The hassles and costs of litigating over hard drive searches and inspections may be easily avoided by basic e-mail management tools and procedures. Most importantly, a

[15] *See, e.g., Antioch Co. v. Scrapbook Borders, Inc*., 210 F.R.D. 645, 652-54 (D. Minn. 2002); *Rowe*, 205 F.R.D. at 433; *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 641-44 (S.D. Ind. 2000); *Playboy Enterprises v. Welles*, 60 F. Supp.2d 1050 (S.D. Cal. 1999).

company's policy should mandate, and the company's technology should allow, that all employee e-mails (including, if plausible, instant messages, and e-mails from employees' laptops, cell phones, PDAs, and home computers)[16] be sent, received, captured, or routed, on a central server or servers, and thereafter archived on easily accessible and searchable storage media.

As such, if an employee deletes e-mail from his mailbox, original copies of that e-mail still will reside in the firm's archived records, and not just possibly on backup tapes. No need will exist for a plaintiff to request access to any individual employees' hard drives during civil discovery, and no reasonable ground will exist for plaintiff to accuse the defendant or its employees of deleting responsive e-mail.

> The costs of responding to discovery of information contained in computer systems can be best controlled if the organization takes steps ahead of time to prepare computer system and users of these systems, for the potential demands of litigation. Such steps include institutionally defined, orderly procedures for preserving and producing relevant documents and data, and establishing processes to collect, store, review, and produce data that may be responsive to discovery requests or required for initial mandatory disclosures. Preparation for electronic discovery can also help the corporation accurately present the cost and burden of specific discovery requests to the court, control the costs of reasonable steps to produce data, and avoid the risk of failing to preserve or produce evidence from computer systems.

The Sedona Principles at 19.

II.

PRESERVATION OF E-MAIL EVIDENCE

A. Duty To Retain E-Mail

A company has an obligation to preserve potentially relevant electronic records in its possession or control in connection with an anticipated litigation or commenced litigation.

[16] If it not feasible to route or capture on the firm's server employee e-mails that were sent or received outside of the firm's server environment, a company should consider prohibiting or limiting such extra-network e-mail altogether.

"The obligation to preserve evidence arises when the 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." *Zubulake v. UBS Warburg LLC*, 2003 WL 22410619 at *2 (S.D.N.Y. Oct. 22, 2003) (*Zubulake IV*) (citations omitted).

A party's obligation to preserve evidence that may be relevant to litigation is triggered once the party has notice that litigation might occur. *See, e.g., Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998). The obligation to preserve electronic evidence exists independent of any preservation order of the court, preservation demand from the opposing party,[17] or discovery demand from the opposing party. *See e.g., Danis v. USN Comm., Inc*., 2000 WL 1694325 at *1, 32-33 (N.D. Ill. Oct. 23, 2000); *Proctor & Gamble Co. v. Haugen*, 179 F.R.D. 622, 631 (D. Utah 1998), *aff'd in part, rev'd in part on other grounds*, 222 F.3d 1262 (10th Cir. 2000).

The duty to preserve electronic evidence must be discharged actively. Senior management must advise employees in possession of discoverable materials of their obligations to preserve documents known to be relevant to the issues in the litigation, or reasonably calculated to lead to the discovery of admissible evidence, or reasonably likely to be requested during discovery, or known to the subject of a pending discovery demand. If the court has entered a preservation order in the case, senior management must provide employees with a copy of the court's order and acquaint them with the potential sanctions that could issue for non-compliance with the order. The company also should implement and distribute to employees a comprehensive written preservation plan with specific criteria for finding and securing relevant electronic evidence for the litigation. The company also must

[17] For an example of an electronic evidence preservation demand, *see Wiginton*, 2003 WL 22439865 at *1.

actively monitor compliance with the preservation plan. *See generally Danis*, 2000 WL 1694325 at *32, 37.[18]

Zubulake IV sets forth a broad and clear standard for preservation of e-mail on hard drives and backup tapes:

> 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. In recognition of the fact that there are many ways to manage electronic data, litigants are free to choose how this task is accomplished. For example, a litigant could choose to retain all then-existing backup tapes for the relevant personnel if such tapes store data by individual or the contents can be identified in good faith and through reasonable effort, and to catalog any later-created documents in a separate electronic file. That, along with a mirror-image of the computer system taken at the time the duty to preserve attaches (to preserve documents in the state they existed at that time), creates a complete set of relevant documents. Presumably there are a multitude of other ways to achieve the same result.
>
> . . . .
>
> The scope of a party's preservation obligation can be described as follows: Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents.[19] As a general rule, that litigation hold does not apply to inaccessible backup tapes (*e.g.*, those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if backup tapes are accessible (*i.e.*, actively used for information retrieval), then such tapes *would* likely be subject to the litigation hold.
>
> However, it does make sense to create one exception to this general rule. If a company can identify where particular employees documents are stored on backup tapes, then the tapes storing the documents of "key players" to the existing or

[18] If the company is a public company, it also should instruct outside directors to preserve relevant documents. *See In re Triton Energy Ltd. Securities Litigation*, 2002 WL 32114464 (E.D. Tex. March 7, 2002); *Danis*, 2000 WL 1694325 at *41.

[19] "Whether a company's duty to preserve extends to backup tapes has been a gray area. As a result, it is not terribly surprising that a company would think that it did *not* have a duty to preserve all of its backup tapes, even when it reasonably anticipated the onset of litigation . . . . Litigants are now on notice, at least in this Court, that backup tapes that can be identified as storing information created by or for the 'key players' must be preserved." *Zubulake* IV, 2003 WL 22410619 at *6 and n.47 (emphasis in original).

> threatened litigation should be preserved if the information contained on those tapes is not otherwise available. This exception applies to *all* backup tapes.[20]

Zubulake IV, 2003 WL 22410619 at *4 (emphasis in original).

The Advisory Committee on Civil Rules presently is considering proposing an amendment to the Federal Rules of Civil Procedure to address a party's duties to preserve electronic evidence. For instance, draft Rule 26(h)(3) provides:

> **Preserving electronically-stored data**. Upon commencement of an action, the parties must preserve electronically-stored data that may be required to be produced pursuant to Rule [26(a)(1) and] (b)(1), except that materials described by Rule 26(h)(2) need not be preserved unless so ordered by the court for good cause. Nothing in these rules requires a party to suspend or alter the operation in good faith of disaster recovery or other [computer] systems (for electronically –stored data) unless the court so orders for good cause, [providing that the party preserved a single day's full set of such backup data].[21]

B. Sanctions for "Spoliation" of E-Mail

Once a party suspects that the other party or its employees have destroyed or otherwise failed to preserve certain e-mail for discovery, it will petition the court to sanction the opposing party for so-called "spoliation" (*i.e.*, destruction) of evidence.

A court has the inherent and statutory powers to impose sanctions against a party for destroying relevant electronic evidence. *See generally Trigon Ins. Co. v. United States*, 204 F.R.D. 277, 284-85 (E.D. Va. 2001). A court is given broad discretion to choose the appropriate sanction for spoliation given the unique factual circumstances of every case. *See generally Id*. at 287-88.

---

[20] *See also Wiginton*, 2003 WL 22439865 at *7 (the court found that defendant acted in "bad faith" by failing to halt routine recycling of backup tapes, because plaintiff had submitted a preservation letter to defendant requesting that it preserve all backup tapes containing relevant e-mails); *Linnen*, 1999 WL 462015 at *8-11 (defendant violated the court's preservation order by failing to suspend the customary recycling of backup tapes for the electronic mail system. Also, after the court's preservation order was vacated, and after being served with a request for documents that reasonably encompassed backup tapes, defendant violated its general duties to preserve documents by failing to suspend recycling of the backup tapes).

[21] The draft rule is referring to a "snapshot" backup tape or tapes of all data on the computer system on the day the defendant becomes aware of the suit.

Sanctions for spoliation typically include one or more of the following: (1) default judgment against the defendant, or conversely, dismissal of plaintiff's action;[22] (2) an "adverse inference instruction" to the jury;[23] (3) additional discovery at responding party's cost; [24] (4) monetary sanctions;[25] and (5) attorneys' fees.[26]

---

[22] This harsh sanction "should only be employed in extreme situations where there is evidence of willfulness, bad faith or fault by the noncomplying party." *Wiginton*, 2003 WL 22439865 at *6 (quotation marks and citation omitted). *See Kucala Enterprises, Ltd. v. Auto Wax Co., Inc.,* 2003 WL 21230605 at *8 (N.D. Ill. May 27, 2003) (dismissal of suit entered against plaintiff company that used a computer program called "Evidence Eliminator" to delete 12,000 files from its owner's desktop computer a few hours before the defendant's computer specialist inspected the computer pursuant to court order), *report and recommendation adopted as modified*, 2003 WL 22433095 (N.D. Ill. Oct. 27, 2003); *Essex Group v. Express Wire Servs*., 578 S.E.2d 705 (N.C. App. Apr. 15, 2003) (default judgment entered after finding that defendant, *inter alia*, intentionally deleted e-mails); *Nartron Corp. v. General Motors Corp.*, 2003 WL 1985261 at *2-5 (Mich. App. Apr. 29, 2003) (dismissal of plaintiff's complaint for, *inter alia*, intentional destruction of computer records), *appeal denied*, 670 N.W.2d 219 (2003).

[23] Such an instruction directs the jury that it can infer from the fact that defendant destroyed certain evidence that such evidence, if available, would have been favorable to the plaintiff and harmful to the defendant. *See, e.g., 3M v. Pribyl*, 259 F.3d 587, 606 n. 5 (7th Cir. 2001)(affirming negative inference instruction where defendant downloaded six gigabytes of music onto his hard drive, overwriting files responsive to plaintiff's demands, on the evening before the computer was turned over for inspection); *Trigon*, 204 F.R.D. at 29 (adverse inference would be drawn respecting the substantive testimony and credibility of the defendant's experts based on their purposeful destruction of e-mails and draft reports).

[24] In *Renda Marine, Inc. v. United States*, 58 Fed. Cl. 57 (Fed. Cl. 2003), a contracting officer for the U.S. Government, after receiving notice of a potential litigation claim by a contractor on one of his projects, continued his regular practice of deleting e-mails concerning the project after sending or responding to them. The court ordered that the government produce at its own expense any back-up tapes created on or after the date of notice of the litigation that might contain the deleted e-mails, and granted the plaintiff access to the officer's hard drive to attempt to recover the deleted e-mails. *See Id.* at 62.

[25] *See, e.g., Proctor & Gamble Co.*, 179 F.R.D. at 632 (defendant sanctioned $10,000 for failing to search and preserve the e-mails of five key employees after the litigation was commenced); *Danis*, 2000 WL 1694325 at *53 (CEO of bankrupt defendant corporation sanctioned $10,000 for failing to implement a suitable document preservation program, thereby leading to the destruction of potentially relevant computerized records).

[26] *Landmark Legal Foundation v. E.P.A.*, 272 F. Supp.2d 70, 87 (D.D.C. 2003) (court ordered defendant to pay plaintiff's legal fees and costs in bringing spoliation motion where defendant violated preliminary court order to preserve documents by reformatting the hard drives of several EPA officials, erasing e-mail backup tapes, and deleting e-mails received after date of order); *Kucala Enterprises, Ltd.*, 2003 WL 21230605 at *8 (award of attorneys' fees and costs incurred from time opposing party first willfully deleted computer files to date of hearing on the spoliation motion); *Trigon*, 204 F.R.D. at 291 (award of attorneys fees and costs incurred as a consequence of spoliation of defendant's expert witness e-mails and draft reports); *Linnen*, 1999 WL 462015 at *13 (award of all fees and costs associated with electronic discovery issues arising from improper recycling of backup tapes during litigation).

Differing circuits have differing requirements for establishing spoliation. As discussed in *Zubulake IV,* in the Second Circuit, a party seeking sanctions based on spoliation of evidence must establish three elements:

> (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a "culpable state of mind" and (3) that the destroyed evidence was "relevant to the party's claim or defense such that a reasonable trier of fact could not find that it would support that claim or defense. . . . [A] "culpable state of mind" for purposes of a spoliation [sanction] includes ordinary negligence. When evidence is destroyed in bad faith (*i.e.*, intentionally or willfully), that fact alone is sufficient to demonstrate relevance. By contrast, when the destruction is negligent, relevance must be proven by the party seeking the sanctions.

Zubulake IV, 2003 WL 22410619 at *6.[27]

Spoliation motions generally take on a life of their own, and in many cases completely subsume the underlying litigation. *See Danis*, 2000 WL 1694325 at * 50 ("By the parties' calculations, they have spent an enormous sum of money litigating the sanctions issue: a collective total of $1,524,762.03. That expenditure has been used solely for the purpose of 'litigating the litigation,' and has not contributed to advancing this case to the disposition on the merits that the parties in this case deserve.").

C. Avoiding Spoliation Claims

To avoid the possibility of spoliation sanctions, and the significant legal fees and costs associated with a spoliation motion, a company must have and follow detailed written procedures concerning evidence preservation.

[27] Courts in other circuits utilize slightly different elements in determining whether to grant a spoliation motion. *See, e.g., Applied Telematics, Inc. v. Sprint Communications Co., L.P.*, 1996 WL 33405972 at *2 (E.D. Pa. Sept. 17, 1996) (in the Third Circuit the "key considerations" are: (1) the degree of fault of the party who destroyed the evidence, (2) the degree of prejudice suffered by the opposing party; and (3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party and, where the offending party is seriously at fault, will serve to deter such conduct by others in the future).

First, a company's policy must ensure that written notification be given to all affected owners, officers, directors, and employees of: (1) the possibility of a future litigation, (2) the filing of an actual litigation, (3) the receipt of a preservation letter from opposing counsel concerning potential or actual litigation, and (4) any court orders concerning document preservation. Such written notification should disclose the names of the parties, the nature of the allegations, the key employees who may maintain relevant records, and the employees and third parties who may be potential witnesses. The notification should attempt to define broadly what information and documents might be potentially relevant to the litigation, and the categories of paper and electronic records that must be preserved that may contain relevant evidence.

The notification must instruct employees that they are prohibited from altering, erasing, or hiding potentially relevant electronic records, and should direct the appropriate personnel (*e.g.*, the IT department) to cease routine recycling of backup tapes that may contain relevant records, if necessary and appropriate. The notification should also advise employees of the possible sanctions attendant to failure to properly preserve evidence. The notification also should provide the names and telephone numbers of the appropriate contact persons in management, the legal department, and outside law firms. The company must then take active steps to ensure that its employees understand and adhere to their document preservation obligations, pending the company's efforts to corral, review, and produce, the relevant files and records.

A company's burdens with respect to e-mail preservation will be eased substantially by existing routine procedures, described in Section I above, which ensure that all e-mails are captured, routed, and stored on easily accessible and searchable media such as WORM disks,

optical devices, and tapes. With such procedures in place, individual employees will be unable to delete from their hard drives what possibly may be the company's only copy of a relevant e-mail, thereby obviating the need or opportunity for hard drive inspection of the company's computers by opposing counsel's computer expert. Further, disaster recovery backup tapes need not be restored and searched at considerable cost, and those tapes may be recycled and overwritten in the normal course of business without fear that possibly relevant e-mails are being erased, thereby saving further substantial costs.[28]

With the proper procedures in place, a company can substantially decrease its litigation-related costs and anxieties. Potentially relevant evidence can be quickly accessed and searched for relevance, and be subject to privilege review. Corporations and their attorneys then can be freed to focus on the merits of the litigation, and on substantive litigation strategy, unburdened by the mind-numbing and cost-intensive aspects of electronic discovery.

D. Additional Considerations

Finally, many companies, large and small, have implemented e-mail policies that require all e-mails, across all business units, to be deleted after a very short time period, *e.g.*, thirty days. The stated rationale for this approach is as follows: if all e-mails are routinely and systematically deleted pursuant to a written company policy, then e-mails will not exist to be discovered in litigation. Such a policy purportedly serves the goals of eradicating potential "smoking-gun" evidence, and reducing, if not eliminating, the potential costs of electronic discovery.

[28] In *Wiginton*, defendant calculated that it would cost the company $12,500 a day for new tapes to replace existing backup tapes that were the subject of discovery and could not be overwritten. *See* 2003 WL 22439865 at *3 and note 3.

This approach is defective because it does not ensure that all copies of internal or external e-mail are actually destroyed. With respect to internal e-mails, employees may download e-mails onto floppy disks, forward them to off-site locations, or print and retain hard copies. With respect to external e-mails, at least one copy will exist on a hard drive or backup tape of a third party over whom the company exercises no control. And, as discussed earlier, e-mails are not instantly "deleted" and cleansed from the company's computer system upon the push of a delete button, but instead they linger on the computer's hard drive as "residual data" until overwritten.

Further, this approach is disastrous for regulated companies that are required to maintain e-mails for a specific period.[29] A thirty-day purging policy also raises serious concerns for public companies under the Sarbanes-Oxley Act of 2002 and the SEC rules issued thereunder, because the policy could have an impact on the company's "internal controls,"[30] and could expose the company to potential criminal charges for obstruction of justice.[31]

---

[29] *See, e.g.*, SEC Release No. 34-46937 (Dec. 3, 2002) (Deutsche Bank, Goldman, Sachs, Morgan Stanley, Salomon Smith Barney, and U.S. Bancorp each fined $1.65 million for failing to maintain all business-related e-mails for three years as required by SEC Rule 17a-4, insofar as these firms systematically discarded, recycled, and overwrote back-up tapes and other storage media containing the e-mails, and/or systematically erased all e-mails on the hard drives of personal computers of departed employees).

[30] Certain companies may not be able to properly maintain internal control over their financial reporting if they fail to review, and otherwise promptly delete, any and all e-mails related to internal accounting. Systematic deletion of all e-mails related to internal accounting might constitute a "material weakness" in a company's internal financial controls under Section 404 of Sarbanes-Oxley, thereby requiring disclosure of such weakness in the company's public filings.

[31] Under Sarbanes-Oxley Section 802, a court may impose a twenty-year prison sentence against a defendant who has destroyed any document (*e.g.*, deleing an e-mail) "in contemplation" of a federal investigation or "matter" that may not yet exist, if that such person's intent was to "impede, obstruct or influence" such future matter. Presuming the inevitability of a federal investigation into the financial activities of any large public company, companies and their officers who adopt policies requiring systematic deletion of all corporate e-mails, within weeks of their creation, for the very purpose of preventing possible adverse evidence from falling into the hands of federal investigators, may be subjecting themselves to possible criminal prosecution and lengthy prison terms.

And finally, and most importantly, the approach represents a head-in-the-sand approach to corporate governance. Simply put, non-management of e-mail is mismanagement of e-mail. And given the central role that e-mail evidence has played in numerous recent major scandals, non-management of e-mail may well be mismanagement of the company itself. The first time senior management learns of misconduct evidenced in a company e-mail should not be when that e-mail is attached as Exhibit A to a multi-million dollar complaint, or when it is reproduced and quoted at length in the Wall Street Journal.