

*“The File is Inside  
the Computer”:  
The Federal Rules  
and a Practical  
Guide to  
Managing  
Discovery of  
Electronically  
Stored  
Information*

February 23, 2009

**Bob Troyer**  
**Sean R. Gallagher**  
Hogan & Hartson LLP  
1200 Seventeenth Street  
Suite 1500  
Denver, Colorado 80202  
303.899.7300

**I. INTRODUCTION****A. THE EXPLOSION OF ELECTRONICALLY STORED INFORMATION**

Technological advancements have exponentially increased the universe of discoverable electronic material, changing the manner in which we must think about electronically stored information ("ESI").

- According to data from the Pew Internet and American Life Project from March 2007, 91% of U.S. Internet users have gone online to send or read e-mail, and 56% do this as part of a typical day.
- There were an estimated 1.2 billion e-mail users in 2007, a number which is expected to rise to 1.6 billion by 2011.
- Some 183 billion e-mails were sent each day in 2006, and wireless e-mail users are estimated to grow from 14 million in 2006, to 228 million in 2010.
- In 2007, the estimated number of business e-mail users was around 780 million.
- According to the Pew Internet Project's December 2007 survey, "58% of adult Americans have used a cell phone or personal digital assistant ("PDA") to do at least one of ten mobile non-voice data activities, such as texting, e-mailing, taking a picture, looking for maps or directions, or recording video." Additionally, "41% of adult Americans have logged onto the Internet on the go, that is, away from home or work either with a wireless laptop connection or a handheld device."
- In 2004, 42% of online Americans used instant messaging, 24% of which reported using instant messaging more frequently than e-mail. This translates to 53 million American adults who instant message and over 12 million who instant message more than e-mail. On a typical day, 29% of instant messengers, nearly 15 million American adults, use instant messaging.
- A single computer tape or small disk drive can hold the equivalent of millions of printed pages.

**B. ELECTRONIC EVIDENCE AND THE FEDERAL RULES**

On December 1, 2006, amendments to the Federal Rules of Civil Procedure went into effect. Many of the amendments address the role of the court and the parties regarding electronic discovery issues. Significantly, the amendments to the rules recognize that electronic files are distinct from paper files and present unique issues that the court and the parties should address at the outset of the litigation process. The 2006 amendments acknowledged that the dynamic nature of electronic data, the inability of some data to be removed from the system on which it resides in any usable form, and a computer system's ability to store enormous amounts of data have created significant difficulties for litigants and courts alike. In addition, they recognize that discovery of electronic information has become extremely time-consuming and expensive, while courts have created a patchwork of discovery rulings and local rules regarding electronic discovery.

The amended rules address these problems by speaking to five significant issues in electronic discovery: (1) the unintentional destruction of electronic data due to a computer system's routine overwrite or recycling of certain data; (2) the accessibility of electronic data; (3) claims of privilege and attorney work product; (4) document preservation; and (5) requests for production of electronically stored information. At a time when storing and managing electronic data is critical to the running of a successful enterprise, companies must be aware of the new rules in order to ensure that electronic document management policies and procedures are in place if and when a company anticipates litigation.

### **The Routine Alteration and Deletion of Electronic Information**

One of the most significant of the 2006 amendments to the Federal Rules of Civil Procedure is the provision regarding potentially discoverable data that is lost because of "the routine alteration and deletion of information that attends ordinary use" of electronic information systems. Amended Fed. R. Civ. P. 37 Advisory Committee Note. Rule 37(f) provides a safe harbor against the sanctions provided by this rule if data is lost as a result of such routine operations and those operations were performed in good faith. This protection, however, is very limited. For instance, the Advisory Committee Notes state that good faith "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." Furthermore, the good faith exception would prohibit a party from exploiting the routine operation of its electronic systems to destroy data it is required to preserve. In addition, the Advisory Committee Notes suggest that good faith might require a party, depending on the circumstances, to take steps "to prevent the loss of information [even] on sources that the party believes are not reasonably accessible" -- even though Rule 26(b)(2)(B) provides that a party need not provide discovery of ESI that is not reasonably accessible because of undue burden or cost. One factor a court could consider in such circumstances "is whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources." Finally, if a judge determines that "exceptional circumstances" exist, he may impose sanctions under Rule 37 if discoverable data is lost because of a system's routine operation even if that operation was in good faith. As a practical matter, the amendments make clear that a "litigation hold" covering potentially discoverable ESI, and intervening in routine destruction, is essential when litigation is pending or reasonably anticipated.

### **Information That Is Not Reasonably Accessible**

Rule 26(b)(2)(B) expressly states that a "party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost." Thus, the responding party must "identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing." Rule 26(b)(2)(B) Advisory Committee Note. Furthermore, this identification should "provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources." Though the Rule and its Advisory Committee Note do not define information "not reasonably accessible," examples of such information may include back-up tapes kept for disaster recovery purposes that are not indexed, information from obsolete legacy systems that cannot be read by current systems, or deleted data that may remain in fragment form on a company's computer systems. However, a party is still bound by common-law and statutory duties of preservation, so a party may still be required to preserve such information.

The idea behind this amendment is that parties should first look to discoverable data that is easily accessed and produced, and only after a review of those materials should they pursue discovery, if necessary, of data that is less accessible. Thus, though there is no initial obligation to provide discoverable information from sources that are not reasonably accessible, a court may still require the production of such information if the requesting party shows “good cause” for the discovery of such information. A party may demonstrate good cause by showing that the need for discovery outweighs the burden or cost to the responding party to retrieve and produce the information. Furthermore, the responding party will bear the burden of proving that the data is not reasonably accessible if the requesting party challenges the identification of certain material as not reasonably accessible. Ultimately, the court will decide the conditions for discovery of such information, including whether to require the requesting party to pay for the expense of retrieving the information.

### **Privilege and Work-Product Claims**

Rule 26(b)(5) acknowledges the risk of inadvertently producing privileged material, given the difficulties in reviewing voluminous electronic records accurately, and provides a mechanism for parties to assert privilege or work-product protection after such documents have been produced. Under Rule 26(b)(5)(B), a party making the claim of privilege may notify the party that received the information of the privilege claim and the basis for it. Upon such notification, the receiving party must promptly “return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved.” In addition, the receiving party must take “reasonable steps” to retrieve the allegedly privileged information if it disclosed such information to non-parties. The Rule allows the receiving party to present the privileged information to a court under seal in order to resolve the dispute. However, it is important to note that the Rule does not provide guidance as to when the privilege will be deemed waived by the production of privileged materials.

The amended rules acknowledge that reviewing and determining the privilege and work-product status of electronic information can be difficult due to the potential volume of discoverable electronic materials and the fact that certain information, such as embedded information or metadata that are not immediately apparent when viewing a document, can contain privileged information. Thus, in addition to the procedure outlined above, Rule 26(f)(3) directs both parties to discuss privilege and work-product issues prior to discovery, with the hope that parties will come to an agreement on “a procedure to assert such claims after production.” The Rule anticipates that such an agreement will save both parties time and expense by allowing parties to review and produce discoverable information more quickly because they will be less concerned about exacting review at the outset. See, e.g., *Containment Technologies Group v. American Soc. of Health System Pharmacists*, 2008 U.S. Dist. Lexis 80688 (S.D. Ind. Oct. 10, 200\*) (approving designations of entire document collection as “confidential” under amended F.R.E. 502).

### **Electronic Document Preservation**

Though the rules do not discuss the exact nature of a party’s preservation responsibility, Rule 26(f) directs parties to discuss the preservation of information, electronic and otherwise, early on in the case, prior to meeting with the judge. The contours of this requirement become important when discoverable electronic information is at issue because electronic data is often dynamic -- and because the costs to compile and preserve this information can be significant. Thus, the Advisory Committee Notes suggest that the parties focus on “the balance between

the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities,” noting that the “[c]omplete or broad cessation of a party’s routine computer operations could paralyze the party’s activities.” The obligation to discuss the preservation of discoverable information is directed at avoiding later disputes regarding preservation issues.

### **Requests for the Production of Electronic Data**

The amendments to the rules also sought to ensure a uniform approach to the discovery of electronic data. For instance, Rule 33(d), regarding the production of business records in response to an interrogatory, specifically includes the production of electronic business records. The Advisory Committee Notes state, however, that in order to meet the requirements of Rule 33(d), the responding party might need to provide “technical support, information on application software, or other assistance” when referring the requesting party to such records. In addition, Rule 34, regarding requests for production, specifically recognizes “electronically stored information” as a distinct category of data, separate from “documents.” Rule 34 also allows a requesting party to request the particular form of production for electronic data. Because a requesting party may not know the forms in which the data is maintained, Rule 26(f)(3) requires that parties discuss the form of production of data in the parties’ pre-discovery conference. If the requesting party fails to identify the form of production, or if the form of production is objected to, the responding party must identify the form in which it intends to produce the data, and the form must be “the form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable.” Rule 34(b)(ii).

### **C. FEDERAL RULE OF EVIDENCE 502**

Driven by the skyrocketing costs of producing electronically stored information in litigation, long-anticipated Federal Rule of Evidence 502 became law in September 2008. Rule 502 is intended to reduce the staggering costs of document and ESI review by protecting against waiver of the attorney-client privilege and work-product protection. The rule applies to proceedings commenced after the effective date and, “insofar as is just and practicable,” to all proceedings pending on that date. Rule 502 seeks to protect against forfeiting a privilege when disclosure in a federal action is the result of an innocent mistake. The rule also gives teeth to court orders permitting procedures like both the so-called “quick peek” that allows requesting parties to look at and assess a producing party’s ESI before more precisely defining the scope of production, and “claw-backs” that allow the return of inadvertent disclosures without waiver.

In complex litigation, lawyers have always spent significant time in efforts to preserve the work product and attorney-client privileges especially because in some jurisdictions, if one protected document is produced -- even inadvertently -- there is always the risk that a court might find a subject-matter waiver. Subject-matter waiver means that privilege are considered waived not only as to the disclosure at issue but also as to all related material -- and not only in that instant case, but in all other cases.

Case law has many examples of inadvertent disclosures of otherwise privileged material due to clerical, vendor, or attorney error. But the real problem is ESI. Our still-adolescent paradigm of electronic data retention, having subsumed the former paper regime, mushrooms the potential for inadvertent production. Problems include the fact that normal viewing of native-format computer documents, for example, will not reveal existing metadata about who wrote, edited or last opened a document. Embedded data (such as that created by Word’s Comment, Track

Changes, and Undo features) do not necessarily appear on the screens of reviewing attorneys. The now-ubiquitous word searches performed using certain native applications, like Outlook, will not identify responsive and potentially privileged attachments. There is also the multiple-replication problem, endemic to ESI, that provides numerous opportunities for one iteration of a privileged document to slip through a privilege review. These problems are of course amplified by the sheer magnitude of sometimes gigabytes or terabytes of data that are increasingly necessary to review in the wake of the now-famous *Zubulake* opinions (discussed below) and the subsequent 2006 civil procedure rule amendments.

Rule 502 tries to address this cost-of-review issue in several ways. First, it provides that, cases of actual waiver will not automatically be deemed subject-matter waivers. Information other than that specifically waived would be produced only if it "ought in fairness" be considered together. The committee note explains that the "fairness" determination required for a broader waiver should be limited to situations where a party intentionally puts information into litigation in a selective, misleading and unfair matter. But any cost savings here would seem to flow only from not having to review and produce many additional documents with an intentionally produced but otherwise privileged document. As to the menacing prospect of inadvertent disclosure, the rule provides that if inadvertent disclosure is made at the federal level, no waiver will be found if the holder has (1) taken reasonable steps to prevent the disclosure and (2) employed reasonably prompt measures to retrieve the mistakenly disclosed information. This provision codifies a middle-ground standard that had been adopted by a plurality of courts requiring some form of balancing test. A minority of courts applied either strict liability -- meaning that any inadvertent disclosure is a waiver, and perhaps a subject-matter waiver -- or intent-based standards that find for no waiver for inadvertent disclosure under the reasoning that a waiver must be knowing and intended. Under Rule 502, state courts in subsequent state proceedings will be required to honor Rule 502 determinations made at the federal level, and if there is an earlier disclosure of privileged or protected information in a state proceeding admissibility in a subsequent federal proceeding will be determined by the law that is most protective against waiver.

Importantly, under the new rule, federal courts are permitted to enter confidentiality orders providing that disclosures of privileged or protected material -- under, for example, quick-peek and claw-back agreements -- do not constitute waivers as to other parties in other state or federal proceedings.

But even a "middle-ground" balancing as to inadvertent disclosure can provide seemingly harsh results. As recently as May 29, 2008, a District of Maryland court applied a common-law balancing test but found waiver for the inadvertent production of 165 privileged documents, out of tens of thousands reviewed, because the party failed to satisfy its burden to establish its search and review methodology was "reasonable." *Victor Stanley, Inc. v. Creative Piope, Inc.*, --- F.R.D.---, 2008 WL 2221841, at \*1-7 (D. Md.). Nor was the magistrate judge in *Victor Stanley* impressed with the producing party's "prompt measures to retrieve the mistakenly disclosed data," as his opinion scolded the party for the "delay" of a "one-week period between production by the Defendants and the time of the discovery by the Plaintiff of the disclosures -- a period during which the Defendants failed to discover the disclosure." *Id.* at \*8.

The Committee Note to Rule 502 does acknowledge that while the rule "does not require the producing party to engage in a post-production review to determine whether any protected communication or information has been produced by

mistake,” it does require follow-up on obvious indications of potential production of protected material. Moreover, regarding whether “reasonable steps” were taken to prevent a disclosure, the Committee Note suggests that using advanced analytical software applications and linguistic tools in screening for privilege may suffice (*i.e.* with no page-by-page attorney review). Further, implementation of an efficient system of records management may also be relevant to a reasonableness determination. In other words, a court may look to steps taken both before litigation and during production even though those steps don’t involve actual attorney review.

#### **D. A LACK OF GUIDANCE**

Until the 2006 amendments to the Federal Rules, judges and attorneys had been struggling with the question of how to deal with the explosion of electronic evidence and with issues relating to its preservation and production (and the associated costs). Courts had generally embraced the concept of expansive electronic discovery. See, e.g., *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 WL 649934, at 2 (S.D.N.Y. 1995) (“[I]t is black letter law that computerized data is discoverable if relevant.”); *Rowe Entm’t, Inc. v. The William Morris Agency, Inc.*, 205 F.R.D. 421, 427-431 (S.D.N.Y. 2002) (noting that “[e]lectronic documents are no less subject to disclosure than paper records,” and only questioning which party should bear the cost of such discovery, especially for backup tapes or deleted e-mails). But they had been developing new rules on an *ad hoc*, often highly fact-specific basis. Now, more than two years after the enactment of the 2006 amendments, the rules are finally becoming clearer for litigants.

## **II. UNIQUE CHARACTERISTICS OF ELECTRONIC EVIDENCE**

### **A. THE DIGITAL TRAIL**

As is discussed in more detail below, the use of electronic communication leaves a distinct digital trail. Consequently, electronic evidence is a particularly fruitful source of evidence, for unlike documents in hard copy form, electronic evidence often provides information that is not readily apparent to the user. In essence, a hard copy file tells only part of the story -- the rest of that story is contained in electronically stored formats. This unique feature of electronic evidence, combined with its proliferation, is having a dramatic impact on the litigation process.

### **B. THE EASE OF REPLICATION**

Electronic documents also are more easily replicated than paper documents. Although paper documents can be copied, electronic data can be replicated on a massive scale without causing the degradation of that data. For instance, e-mail users often send the same message to several recipients who, in turn, may forward that message along to others. While these transmissions are taking place, the underlying software automatically creates multiple copies of the sent and received e-mails. Similarly, other common software applications are often designed to periodically and automatically make copies of data to protect against deletion, or for other purposes.

### **C. THE DELETION FALLACY**

Electronic documents also are much more difficult to dispose of than paper documents. One of the most common fallacies in relation to electronic evidence is the notion that once an e-mail or document is deleted, it can never be recovered. In fact, deleted documents may often be recovered in whole or in fragments long

after their deletion. Generally speaking, the more recent the deletion, the more likely a document will be successfully recovered. Important to note, however, is the fact that even files that have been deleted and overwritten may be found in other places on a computer's hard drive, referred to as "free space" or "slack space," and those files can be the source of relevant information. See, e.g., *State v. Townsend*, 57 P.3d 255 (Wash. 2002) (noting that "[a]lthough some e-mail services may offer the possibility of 'shredding' an e-mail message, arguably the equivalent of actually deleting it, the e-mail file may still be retrievable using certain software. 'A deleted file is really not a deleted file, it is merely organized differently.'"); *Adobe Sys., Inc. v. Sun South Prod., Inc.*, 187 F.R.D. 636 (S.D. Cal. 1999) ("Manual or automated deletion of that software may remove superficial indicia.... However, telltale traces of a previous installation remain, such as abandoned subdirectories, libraries, information in system files and registration keys....").

### III. TYPES OF ELECTRONICALLY STORED INFORMATION: THE COMPONENTS OF THE DIGITAL TRAIL

#### A. WORD PROCESSING DOCUMENTS / E-MAIL & BACKUP TAPES

Word processing documents and e-mail messages contain the information we normally associate with hard copy documents, which is the user-created content. Important to note is the fact that this user-created electronic content is generally transferred to backup media of some kind on a regular basis.

#### B. METADATA

##### 1. Definition

Metadata is information that characterizes data, answering the questions who, what, when, where, why and how about the data being documented. It consists of the thousands of pieces of information that are automatically created and maintained by software programs, and it reveals the following types of information, distinct from the user-created content of the file:

- o creation, edit, comment and deletion dates and times; and
- o authorship or username associated with those tasks.

It is metadata that reveals, for example, the blueprint of a back-dated document -- or a party's improper attempts to delete relevant information after receiving notification of a lawsuit.

##### 2. Metadata Associated With Document Types

- a. **Word Processing Documents:** In addition to tracking authorship, creation and modification dates and times, metadata associated with Word documents enables the "undo" function, which allows for the recall of deleted information. Word processing document metadata also contains hidden codes that determine when to indent a paragraph, change a font, and set line spacing.

- b. **E-mail Messages:** E-mail messages have their own metadata elements that include, among 800 or more properties, information such as:
  - “to”, “from,” “cc” and “bcc” information;
  - dates and times e-mails were sent, received, replied to and forwarded; and
  - sender address-book information.
- c. **Spreadsheets:** Spreadsheets may contain hidden calculations or hidden columns not visible in hard copy versions.
- d. **Internet documents:** Internet documents contain hidden data or “meta-tags” that allow for the transmission of information between an Internet user’s computer and the server on which the Internet document is contained. These “meta-tags” allow search engines to locate websites responsive to specified search criteria.

#### C. EMBEDDED DATA

“Cookies” are metadata containing embedded codes that can be placed on a computer accessing the Internet, without user knowledge. Those codes can, among other things, track usage and transmit information back to the originator of the cookie.

#### D. REPLICANT DATA

Replicant data, which exists in the form of cache and history files, includes:

- data that a computer system automatically records, and that will remain even after the original document has been purged from the system; and
- information copied to removable media in order to provide users with access to data in the event of a system failure.

#### E. RESIDUAL DATA

Residual data is data that has been deleted from the system but continues to reside on the hard drive until overwritten by another file. Depending on the size and use of the computer system, it may take weeks or even months to overwrite the space containing the “deleted” information.

### IV. CASE LAW UPDATE

#### A. ZUBULAKE SET THE STAGE

The starting point for any discussion of discovery of ESI is a garden-variety sex discrimination case brought against UBS Warburg, LLC. In *Zubulake v. UBS Warburg, LLC*, U.S. District Judge Shira Scheindlin foreshadowed many of the 2006 amendments when she crafted a series of thoughtful decisions addressing

the electronic evidence retention and search obligations of a defendant in civil litigation. See *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) (“*Zubulake I*”); *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003) (“*Zubulake II*”); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003) (“*Zubulake IV*”); *Zubulake v. UBS Warburg LLC*, 2004 WL 1620866 (S.D.N.Y. 2004) (“*Zubulake V*”). Although the *Zubulake* decisions came before the 2006 amendments, and are not necessarily binding in other jurisdictions, Judge Scheindlin’s analysis continues to be cited in many post-amendment decisions. For example, Judge Scheindlin’s analysis of when a duty to preserve ESI arises has often been cited in cases on that topic. In *Zubulake IV*, Judge Scheindlin held 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. 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.”

220 F.R.D. at 218.

In *Zubulake V*, Judge Scheindlin summarized a client’s and counsel’s obligations with regard to the production of electronic evidence. Those duties are as follows:

- Counsel’s duty to locate relevant information.

“Once a litigation hold is in place, a party and its counsel must make certain that all sources of potentially relevant information are identified and placed ‘on hold.’ To do this, counsel must become fully familiar with her client’s document retention policies, as well as the client’s data retention architecture. [citations omitted] This will invariably involve speaking with information technology personnel, who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm’s recycling policy. It will also involve communicating with the ‘key players’ in the litigation, [citations omitted] in order to understand how they stored information.” *Id.*

- Counsel’s continuing duty to ensure preservation.

“Once a party and her counsel have identified all of the sources of potentially relevant information, they are under a duty to retain that information (as per *Zubulake IV*) and to produce information responsive to the opposing party’s requests. Rule 26 creates a ‘duty to supplement’ those responses. . . . The *continuing* duty to supplement disclosures strongly suggests that parties also have a duty to make sure that discoverable information is not lost. . . . At some point, the client must bear responsibility for a failure to preserve. At the same time, counsel is more conscious of the contours of the preservation obligation; a party cannot reasonably

be trusted to receive the 'litigation hold' instruction once and to fully comply with it without the active supervision of counsel.<sup>1</sup> . . . There are thus a number of steps that counsel should take to ensure compliance with the preservation obligation. . . . *First*, counsel must issue a 'litigation hold' at the outset of litigation or whenever litigation is reasonably anticipated. . . . *Second*, counsel should communicate directly with the 'key players' in the litigation, *i.e.*, the people identified in a party's initial disclosure and any subsequent supplementation thereto. . . . *Finally*, counsel should instruct all employees to produce electronic copies of their relevant active files." *Id.*

## B. GENERAL DISCUSSION OF ELECTRONIC DISCOVERY

- *DE Techs., Inc. v. Dell, Inc.*, 2007 WL 128966 (W.D. Va. 2007) (finding defendant's production of electronic documents satisfied the requirement that such documents be "produced as kept in the normal form of business" because Fed. R. Civ. P. 34(b) does not require documents be produced in an "*identical* format" but rather be "reasonably usable")
- *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 2008 WL 2221841 (D. Md. 2008) (finding that the privilege covering 165 electronically stored documents was waived because the producing defendant failed to run a reasonable keyword search or conduct quality-assurance testing)
- *United States v. O'Keefe*, 537 F. Supp. 2d 14, 24 (D.D.C. 2008) (discussing the challenges and potential costs that arise when conducting keyword searches in electronic record files for discovery purposes, as such searches involve the "interplay at least, of the sciences of computer technology, statistics and linguistics.")

## C. PRIVILEGE LOGS

- *Baxter Healthcare Corp. v. Fresenius Medical Care Holding, Inc.*, Case No. 3:07-cv-01359, \_\_\_ F. Supp. \_\_\_ (N.D.Cal. October 10, 2008) (ordering defendants to produce "a full and accurate privilege log that separately identifies the author, recipient(s), copy(s), and blind carbon copy(s) for each logged e-mail communication regardless of whether the communication is part of an e-mail string")

## D. COURT-ORDERED PRESERVATION

### 1. Backup Tapes

- *Consol. Aluminum Corp. v. Alcoa, Inc.*, 244 F.R.D. 335 (M.D. La. 2006) (reasoning that while the general rule is a litigation hold does not apply to inaccessible backup tapes, if such

<sup>1</sup> Judge Scheindlin further noted that "[w]hile, of course, it is true that counsel need not supervise every step of the document production process and may rely on their clients in some respects," [citation omitted] counsel is responsible for coordinating her client's discovery efforts. In this case, counsel failed to properly oversee UBS in a number of important ways, both in terms of its duty to locate relevant information and its duty to preserve and timely produce that information." 220 F.R.D. at 218.

backup tapes are accessible [actively used] then they would likely be subject to a litigation hold)

- *Zhou v. Pittsburgh State University*, 2003 WL 1905988 (D. Kan. Feb. 5, 2003) (holding that “the disclosing party must take reasonable steps to ensure that it discloses any back-up copies of files or archival tapes that will provide information about any ‘deleted’ electronic data”, and ordering that the defendant disclose all data compilations, computerized data and other electronically-recorded information)
- *Renda Marine v. United States*, 58 Fed.Cl. 57 (Fed. Cl. 2003) (holding that defendant’s legal obligation to preserve evidence upon notice that litigation might occur extended to its back-up tapes created before and after notice of the litigation)
- *McPeck v. Ashcroft*, 202 F.R.D. 31, 33 (D.D.C. 2001).
  - stating that “during discovery, the producing party has an obligation to search available electronic systems for information demanded,” and ordering a limited back-up restoration of e-mail messages.
  - noting that “[t]here is certainly no controlling authority for the proposition that restoring all backup tapes is necessary in every case. The Federal Rules of Civil Procedure do not require such a search, and the handful of cases are idiosyncratic and provide little guidance.”

## 2. Meta and Other Embedded Data

- *Palgut v. City of Colo. Springs*, 2007 WL 4277564 (D. Colo. 2007) (holding that the “trigger date” by which defendant had a duty to preserve information was upon receipt of a litigation hold letter from plaintiff’s counsel, as opposed to a later date on which the initial complaint was served)
- *United States v. O’Keefe*, 537 F. Supp. 2d 14 (D.D.C. 2008) (requiring plaintiff to preserve electronically stored information in its native format with metadata pending the court’s decision as to whether electronically stored information produced without metadata violates Fed. R. Civ. P. 34(b) and is not “reasonably useable”)
- *In re Verisign, Inc. Sec. Litig.*, 2004 WL 2445243 (N.D. Cal. Mar. 10, 2004) (affirming a magistrate judge’s order that all documents be produced in their native (.pst) format instead of being produced as a (.tiff) image, while recognizing that “it may be difficult for Defendants to incorporate their redactions and bates numbers into the .pst format, but it is not convinced that the responsive documents are so replete with privilege redactions that such a task would transcend all reasonableness”)

- *Positive Software Solutions v. New Century Mortgage Corp.*, 259 F. Supp. 2d 561 (N.D.Tex. 2003) (denying plaintiff's motion to require defendant to image "all of Defendants' media potentially containing any of the software and electronic evidence relevant to the claims in this suit" and "all images of [Defendants'] computer storage facilities, drives, and servers taken to date" on grounds that it was overbroad, in part because it would have required imaging of everything on the server, including irrelevant or privileged information)
- *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 652 (D. Minn. 2002) ("[I]t is a well accepted proposition that deleted computer files, whether they be e-mails or otherwise, are discoverable.")
- *Simon Property Group v. mySimon, Inc.*, 194 F.R.D. 639, 640 (S.D. Ind. 2000) (noting that computer records, including files that had been "deleted," are discoverable documents)
- *Kleiner v. Burns*, 48 Fed. R. Serv. 3d 644, 2000 WL 1909470, at \*4 (D. Kan. Dec. 15, 2000) (concluding that "[t]he disclosing party shall take reasonable steps to ensure that it discloses any backup copies of files or archival tapes that will provide information about any 'deleted' electronic data")

### 3. Transient Data

- *Columbia Pictures Indus. Inc. v. Bunnell*, 2007 U.S. Dist. LEXIS 46364 (C.D. Cal. 2007) (ordering preservation of server log data stored in random access memory as it was "extremely relevant" under Fed. R. Civ. P. 34 and the preservation of such data was not unduly burdensome)
- *Smith v. Café Asia*, 2007 U.S. Dist. LEXIS 73071 (D.D.C. 2007) (requiring plaintiff to preserve images on his cell phone pending a determination of potential privacy issues)

## E. COURT-ORDERED PRODUCTION

### 1. Back-up Tapes

- *U & I Corp. v. Advanced Med. Design, Inc.*, 2007 WL 4181900 (M.D. Fla. 2007) (postponing plaintiff's request for a protective order pending receipt of an affidavit from plaintiff explaining why requested backup tapes were "unloadable")
- *Kaufman v. Kinko's Inc.*, 2002 WL 32123851, at \*2 (Del.Ch., Apr. 16, 2002) (ordering production of e-mails retrievable from defendant's back-up system and stating that "[u]pon installing a data storage system, it must be assumed that at some point in the future one may need to retrieve the information previously stored. That there may be deficiencies in the retrieval system... cannot be sufficient to defeat an

otherwise good faith request to examine the relevant information.”)

- *Renda Marine v. United States*, 58 Fed.Cl. 57 (Fed. Cl. 2003) (ordering defendant to produce, at its expense, back-up tapes created after notice of litigation; to provide plaintiff with access to a requested hard drive; and to produce back-up tapes predating notice of the suit at the plaintiff’s expense)
- *Superior Consultant Co. v. Bailey*, 2000 WL 1279161 (E.D. Mich. Aug. 22, 2000) (ordering defendant to create and produce for plaintiff a back-up file of defendant’s laptop computer, and a back-up file of any personal computer hard drive to which defendant had access)

## 2. Meta / Replicant / Embedded Data

- *In re Honza*, 242 S.W.3d 578 (Tex. App. 2008) (rejecting defendants’ attempt to set aside order requiring production of defendants’ hard drives for imaging by a computer forensic expert to locate metadata of two documents serving as the underlying basis for the lawsuit)
- *Butler v. Kmart Corp.*, 2007 WL 2406982 (N.D. Miss. 2007) (ordering that defendant produce responsive electronically stored information or, if no such evidence exists, a response confirming a diligent search of its computer systems, but denying plaintiff’s request for direct access to defendant’s databases)
- *Giardina v. Lockheed Martin Corp.*, 2003 WL 1338826 (E.D. La. Mar. 14, 2003) (ordering production of a list of all “non-work related internet sites” accessed via sixteen different company computers despite defendant’s objection that the request was overly broad and burdensome)
- *Taylor v. State*, 93 S.W.3d 487 (Tex. App. 2002) (agreeing with defendant’s argument on appeal that he should have been provided with a complete copy of the hard drive in question because “mere inspection of the images... is not the same as inspection of the drive itself (or an exact copy thereof). It is certainly not the same as an independent forensic examination of the contents of the drive by an expert.”)

## 3. Residual Data

- *Peskoff v. Faber*, 224 F.R.D. 54 (D.D.C. 2007) (ordering parties to collect bids from forensic computer technicians for an examination of the parties’ computers for deleted or misplaced e-mails sent to and received by plaintiff)
- *Benton v. Dlorah, Inc.*, 2007 WL 3231431 (D. Kan. 2007) (granting defendant’s request to compel production of plaintiff’s personal computer for inspection by a forensic expert)

in order to recover relevant e-mails deleted by plaintiff, limiting the scope of discovery to topics pertinent to the case)

- *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 652 (D. Minn. 2002) (“[I]t is a well accepted proposition that deleted computer files, whether they be e-mails or otherwise, are discoverable.”)
- *Easley, McCaleb & Assoc., Inc. v. Perry*, No. E-2663 (Ga. Sup. Ct. July 13, 1994) (ordering discovery of deleted files from defendant’s hard drive and allowing plaintiff’s expert to retrieve all recoverable files)
- *Simon Property Group v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. 2000) (holding plaintiff entitled to recover deleted computer files from computers used by defendant’s employees)
- *Playboy Enterprises Inc. v. Wells*, 60 F.Supp. 2d 1050, 1055 (S.D. Cal. 1999) (allowing plaintiff to make a “mirror image” of defendant’s hard drive to recover deleted e-mails)
- *Gates Rubber Co. v. Bando Chemical Industry Ltd.*, 167 F.R.D. 90 (D. Colo. 1996) (allowing plaintiff to copy hard drive to attempt to retrieve information regarding files that defendant’s employee admitted he had deleted)

#### 4. Digital vs. Analog

- *Pamlab, L.L.C. v. Rite Aid Corp.*, 2004 WL 2358106 (E.D.La. Oct. 13, 2004) (holding that if certain prescription information can only be obtained manually it is unduly burdensome, but that if information can be obtained from computer system, it must be produced)
- *Milwaukee Police Assoc. v. Jones*, 615 N.W.2d 190 (Wis. Ct. App. 2000) (concluding that the City’s production of an analog tape of state records was insufficient when a digital version existed, and reasoning that “[a] potent open records law must remain open to technological advances so that its statutory terms remain true to the law’s intent”)

#### 5. Cost Shifting

- *Semsroth v. City of Wichita*, 239 F.R.D. 630 (D. Kan. 2006) (setting forth factors considered in determining whether cost-shifting for data retrieval is appropriate: (1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production, compared to the amount in controversy; (4) the total cost of production, compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issues at stake in the litigation;

and (7) the relative benefits to the parties of obtaining the information)

- *Hutchens v. Hutchen-Collins*, 2007 WL 319990 (D. Ore. 2007) (holding that costs incurred for defendant's expert to authenticate disputed documents on the plaintiff's website were not recoverable under 28 USC § 1920 because they were beyond the cost of copying and the statutory \$40.00 per day witness fee)
- *Paul v. USIS Comm. Svs., Inc.*, 2007 U.S. Dist. LEXIS 68474 (D. Colo. 2007) (denying defendant's motion for reimbursement of preservation costs associated with electronically stored information)
- *Kemper Mortg., Inc. v. Russell*, 2006 WL 2319858 (S.D. Ohio 2006) (denying plaintiff's request that defendant bear the cost of preservation of evidence where plaintiff's counsel had been advised by a computer forensic expert to effect a "litigation hold" by mirroring plaintiff's corporate server, where parties were unable to agree on a protocol for the litigation hold, and where defendant had not proceeded in mirroring plaintiff's server because of the cost involved)
- *Henry v. Quicken Loans, Inc.*, 2008 WL 474127 (E.D. Mich. 2008) (ordering defendant to pay for costs generated by additional e-mail searches conducted by plaintiff's computer forensic expert which were requested by defendant's attorney without plaintiff's knowledge or consent)
- *Rowe Entm't, Inc. v. The William Morris Agency, Inc.*, 205 F.R.D. 421, 429 (S.D.N.Y. 2002) (setting forth the following eight factors for determining whether to shift the cost of data retrieval: (1) the specificity of the discovery requests; (2) the likelihood of discovering critical information; (3) the availability of such information from other sources; (4) the purposes for which the responding party maintains the requested data; (5) the relative benefit to the parties of obtaining the information; (6) the total cost associated with production; (7) the relative ability of each party to control costs and its incentive to do so; and (8) the resources available to each party)
- *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) ("Zubulake I") (setting forth alternate factors for determining whether to shift the cost of data retrieval: (1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production, compared to the amount in controversy; (4) the total cost of production, compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issues at stake in the litigation; and (7) the relative benefits to the parties of obtaining the information)

- *Wiginton v. CB Richard Ellis, Inc.*, 2004 WL 1895122 (N.D.Ill. Aug. 10, 2004) (applying a slightly modified version of the Zubulake factors, the court found that the plaintiff should bear 75% of the discovery costs of restoring the defendants' back-up tapes)
- *Toshiba America Electronic Components, Inc. v. Superior Court*, 124 Cal. App. 4<sup>th</sup> 762 (Cal. App. 2004) (concluding that under the California civil discovery act, the expense of translating a data compilation into usable form should be borne by the requesting party; however, the trial court has discretion to determine the reasonableness of expenses shifted)
- *Peskoff v. Faber*, Case No. 04-526 (D. D.C. July 7, 2008) (responding party must bear the cost of a forensic examination where the need for forensic examination is directly attributable to what was and was not done by the responding party)

## F. COURT REFUSAL TO COMPEL PRESERVATION OR PRODUCTION

Several recent cases indicate that it is possible for litigants to convince courts that the burden of the preservation or production of electronic evidence outweighs its benefit.

### 1. Preservation

- *Cache Le Poudre Feeds, LLC v. Land O'Lakes, Inc.*, 244 F.R.D. 614 (D. Colo. 2007)
  - finding defendants' duty to preserve evidence commenced when the complaint was filed and was not triggered by pre-filing correspondence from plaintiff's counsel, as it did not threaten litigation.
  - holding that a party's obligation to identify and preserve relevant materials in complying with electronic discovery requests "does not automatically include information maintained on computer back-up tapes."
- *John B. v. Goetz*, 531 F.3d 448 (Tenn. 2008) (finding that forensic imaging and production of hard drives as a means to preserve electronic evidence should only be employed where there is a real danger of evidence destruction and no available alternatives)
- *Smith v. Texaco, Inc.*, 951 F.Supp. 109 (E.D. Tex. 1997), *rev'd on other grounds*, 263 F.3d 394 (5th Cir. 2001) (permitting the deletion of electronic records kept in the ordinary course of business provided that hard copies be made and kept)
- *In re St. Jude Med. Inc., Silzone Heart Valve Prod. Liab. Litig.*, 2002 WL 341019, at \*1 (D. Minn. Mar. 1, 2002) (ordering party to preserve newly created documents during the pendency of the case but instructing that the duty to preserve such

documents did not extend to draft or interim versions of documents if they would not have been preserved in the ordinary course of business)

## 2. Production

- *Balfour Beatty Rail, Inc. v. Vaccarello*, 2007 WL 169628 (M.D. Fla. 2007) (refusing to order production of defendants' hard drives where plaintiff's requests were overbroad and failed to make a showing that would justify granting access to the hard drives, such as defendants' non-compliance with discovery rules)
- *Ross v. Abercrombie & Fitch Co.*, 2008 U.S. Dist. Lexis 87039 (S.D. Ohio Oct. 27, 2008) (refusing to order production of 95,000 documents located by new search terms in addition to over one million already produced where plaintiff failed to show that the cost to review and produce more documents was outweighed by the likely relevance of the additional documents to key issues in the case)
- *Williams v. Sprint/United Mgmt. Co.*, 2007 WL 328791 (D. Kan. 2007) (refusing to order defendant to produce documents in the particular form requested by plaintiffs if defendant no longer had the document)
- *Palgut v. City of Colo. Springs*, 2007 WL 4277564 (D. Colo. 2007) (refusing to order restoration of old back-up tapes where defendant had already produced 23,000 pages of discovery in either PDF or ESI format, and where defendant did not have the necessary hardware to access such back-up tapes)
- *Hubbard v. Potter*, 247 F.R.D. 27 (D.D.C. 2008) (finding the "theoretical possibility" that other electronic documents might exist did not warrant additional electronic discovery, and more than speculation on behalf of plaintiff was needed to compel supplemental production)
- *Best Buy Stores, L.P. v. Developers Diversified Realty Corp.*, 247 F.R.D. 567 (D. Minn. 2007) (vacating order that plaintiff restore and produce an electronic database prepared for a separate litigation because the database was not "reasonably accessible" due to the high cost associated with back-up tape restoration and the lack of "good cause" for production)
- *Jones v. Goord*, 2002 WL 1007614 (S.D.N.Y. May 16, 2002)
  - refusing to compel the defendant to produce its databases in electronic form because the burden of the proposed discovery outweighed its likely benefit, particularly in light of the plaintiff's failure to seek discovery in a timelier manner and the vast amount of material that had already been produced in hard copy.

- the plaintiffs in this case, who were prison inmates bringing suit against the New York State Corrections Commission for prison overcrowding, had argued that the electronic information would be more valuable because it would be more manipulable.
- *Torrington Co. v. United States*, 786 F.Supp. 1027 (Ct. Int'l Trade 1992) (refusing to order defendant to create computer tapes from scratch where the plaintiff already received the documents in paper form)
- *Williams v. Owens-Illinois, Inc.*, 665 F.2d 918 (9th Cir. 1982) (refusing to order production of electronic information on computer tape where all data had been previously produced in hard copy)
- *Concord Boat Corp. v. Brunswick Corp.*, 1996 WL 33347247 at \*2, \*9 (E.D. Ark. Dec. 23, 1996) (rejecting as “extremely burdensome” plaintiff’s request to discover all of defendant’s electronic data, which included deleted and archived data, for the previous five years)
- *McCurdy Group v. American Biomedical Group*, 9 Fed. Appx. 822, 831 (10th Cir. 2001) (affirming denial of motion to compel production of hard drives based on fact that party seeking discovery was “skeptical” that all relevant and non-privileged documents had been produced)
- *Strasser v. Yalamanchi*, 669 So. 2d 1142, 1144 (Fla. Ct. App. 1996) (“Even if plaintiff represents accurately that defendant has been thwarting the discovery process, such conduct does not necessarily invite intrusive discovery where there has been no evidence to establish any likelihood that the purged documents can be retrieved.”)

#### **G. INCOMPATIBLE TECHNOLOGY**

As the Advisory Committee Notes to F.R.C.P. 34 make clear, when data can only be made usable by the discovering party through respondent’s devices, the respondent may be required to use its devices to translate the data into usable form. In many instances, this may mean that the respondent will have to supply hard copy versions of electronic data, and the court may allow the discovering party to review the electronic source itself. If the court orders the respondent to allow access to the electronic source of the data, it may protect the respondent with respect to the preservation of the records, the confidentiality of non-discoverable matters, and costs. See, e.g., *Sattar v. Motorola, Inc.*, 138 F.3d 1164 (7th Cir. 1997) (noting that because plaintiff was unable to read defendant’s electronic files, a reasonable accommodation included some combination of downloading data from back-up tapes to conventional disks or a hard drive, loaning plaintiff a copy of the necessary software, or offering plaintiff on-site access to the system).

**V. RAMIFICATIONS OF A FAILURE TO ADEQUATELY PROTECT ESI****A. SANCTIONS**

Several individuals and organizations have been subjected to sanctions for failing to preserve or produce electronic information. The following is a sampling of several of those cases.

- *Nursing Home Pension Fund v. Oracle Corp.*, Case No. 01-00988 SI, (N.D. Cal. 9/2/08) (imposing sanctions on CEO for “willful” destruction of e-mails and other evidence that would have been relevant in shareholder class action against the company)
- *Atlantic Recording Corp. v. Howell*, No. 06-2076 (D. Az. 8/29/08) (default judgment is the appropriate sanction in copyright infringement case against defendant who “repeatedly destroyed evidence central to the factual allegations in the case”)
- *Qualcomm Inc. v. Broadcom Corp.*, 2008 WL 66932 (S.D. Cal. 1/7/08) (court awards sanctions of \$8.5 million in attorneys fees where court found that “one or more of the retained lawyers chose not to look in the correct locations for the correct documents,” accepted “unsubstantiated assurances” from the client that its search was adequate, ignored warning signs that the client’s search was inadequate, or actually encouraged the client to provide false information)
- *Cache Le Poudre Feeds, LLC v. Land O’Lakes, Inc.*, 244 F.R.D. 614 (D. Colo. 2007) (imposing sanctions of \$5,000 for defendant’s failure to preserve potentially relevant data by wiping clean computer’s hard drives and by failing to properly monitor the electronic discovery process)
- *Consol. Aluminum Corp. v. Alcoa, Inc.*, 244 F.R.D. 335 (M.D. La. 2006) (denying plaintiff’s request for monetary sanctions because defendant did not willfully destroy evidence, and instead imposing sanctions requiring defendant to pay plaintiff’s costs and fees for re-deposing witnesses)
- *Coleman (Parent) Holdings Inc. v. Morgan Stanley, Inc.*, 2005 WL 674885 (Fla.Cir.Ct. 2005) (overturned on other grounds, 2007 WL 837221 (Fla. App. 2007) (granting “death knell” adverse inference instruction for failure to preserve and search back-up tapes))
- *Zubulake v. UBS Warburg LLC*, 2004 WL 1620866 (S.D.N.Y. 2004): (“*Zubulake V*”) (granting adverse inference jury instruction on content of deleted e-mails, and ordering defendant to pay for the re-depositions of relevant personnel, the restoration and production of back-up tapes, and the “reasonable expenses, including attorney’s fees,” incurred by plaintiff. Jury subsequently reached \$19 million verdict based on adverse inferences.)
- *United States v. Philip Morris USA Inc.*, 327 F.Supp.2d 21 (D.D.C. 2004) (ordering the defendants to pay costs relating to spoliation as

well as \$2,750,000 in monetary sanctions for failing to stop routine e-mail destruction post-preservation order)

- *Arista Records, Inc. v. Sakfield Holding Co. S.L.*, 314 F.Supp.2d 27 (D.D.C. 2004) (finding that plaintiffs' expert determined that a program designed to erase electronically stored information had been run over 50 times from a remote location in an effort to erase all electronic information on the servers after the plaintiff had asserted copyright infringement claims, and granting plaintiff the right to file appropriate motions for sanctions)
- *Attorney Grievance Comm'n of Maryland v. Potter*, 844 A.2d 367 (Md. 2004) (imposing 90-day suspension from practice on lawyer who intentionally deleted client files from his former law firm's computer system)
- *Renda Marine v. United States*, 58 Fed.Cl. 57 (Fed. Cl. 2003) (holding that the government would be required to produce at its expense back-up tapes that were created on and after date it had notice that litigation might occur and to provide contractor with access to contracting officer's hard drive)
- In August 2002, the SEC fined Citigroup's Salomon Smith Barney Holdings, Morgan Stanley, the Goldman Sachs Group, and others \$10 million for failing to produce e-mails in the course of SEC investigations.
- *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99 (2d Cir. 2002) (ordering trial court to impose sanctions on a corporate litigant for failing to produce e-mail evidence for trial, even though the corporation claimed its expert was having difficulty locating the desired e-mails from its back-up tapes)
- *Procter & Gamble Co. v. Haugen*, 179 F.R.D. 622 (D. Utah 1998), *aff'd in part and rev'd in part on other grounds*, 222 F.3d 1262 (10th Cir. 2000) (imposing sanctions of \$10,000 for the company's failure to search or preserve e-mails of five key employees whom the company itself had identified as having relevant data)
- *Illinois Tool Works, Inc. v. Metro Mark Prod. Ltd.*, 43 F.Supp.2d 951 (N.D. Ill. 1999) (ordering defendant to produce for inspection its computer after plaintiff showed defendant had been less than forthcoming in producing hard copies of requested documents, and ordering sanctions in the form of reasonable attorneys' fees and costs for failure to comply with discovery orders)

## **B. THE SARBANES-OXLEY ACT**

Under Section 802 of the Sarbanes-Oxley Act, companies that fail to retain certain records for a five-year period or who knowingly alter, destroy, mutilate, conceal, or falsify any record, document, or tangible object with the intent to impede, obstruct, or influence proceedings involving federal agencies or bankruptcy proceedings can be subject to criminal liability and even imprisonment.

**VI. PRACTICE TIPS FOR ELECTRONIC DATA RETENTION****A. WHEN MUST THE COMPANY PRESERVE ELECTRONIC DATA?**

Duty to preserve may arise even before a complaint is filed. It arises when the company has “noticed that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.” *Zubulake IV*, 220 F.R.D. at 216-217.

**B. WHAT MUST BE PRESERVED?**

The company is not under a duty to keep every piece of paper, but 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.” *Zubulake IV*, citing *Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D. 68, 72 (S.D.N.Y. 1991). The reasoning in *Zubulake* was applied in *John B. v. Goetz*, 531 F.3d 448, 459 (Tenn. 2008), where the court held a party has the duty to preserve all relevant [electronic] information when that party “has notice that the evidence is relevant to litigation . . . or should have known that the evidence may be relevant to future litigation.” (citing *Fujitsu Ltd. v. Fed. Express Corp.*, 247 F.3d 423, 436 (2d Cir. 2001); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216-18 (S.D.N.Y. 2003)).

**C. DETERMINE WHAT DOCUMENTS ARE ACCESSIBLE OR INACCESSIBLE.**

Whether demanding electronic data in discovery or objecting to a request for ESI as unduly burdensome, the accessibility or inaccessibility of the ESI is the primary question. The court in *Zubulake I* categorized the following electronic data as typically accessible: (1) active, on-line data; (2) near-line data; and (3) off-line storage/archives. The court also characterized the following as less accessible or inaccessible: (1) back-up tapes and (2) erased, fragmented or damaged data.

The court in *W.E. Aubuchon Co., Inc. v. BeneFirst, LLC*, 245 F.R.D. 38, 42 (D. Mass. 2007) employed the categories specified by the *Zubulake* court and listed those categories in the order of most accessible to least accessible: (1) active on-line data (e.g., hard drives); (2) near-line data (typically, robotic storage devices such as optical disks); (3) offline storage/archives (removable optical disks or magnetic tape media which can be labeled and stored in a shelf or rack); (4) back-up tapes; and (5) erased, fragmented or damaged data (such data can only be accessed after significant processing).

**D. WHOSE DOCUMENTS MUST BE RETAINED?**

The duty extends to any employee likely to have relevant information. In *Zubulake IV*, the court characterized this as the “key players” in the case. *Zubulake IV*, 220 F.R.D. at 217-218. The court in *Consol. Aluminum Corp. v. Alcoa, Inc.*, 244 F.R.D. 335, 339 (M.D. La. 2006) also utilized the “key players” language found in *Zubulake IV*, finding a corporation’s duty to preserve extends to employees “likely to have relevant information, i.e. ‘key players’ in the litigation.”

**E. WHAT ARE SUGGESTED METHODS FOR RETAINING DOCUMENTS?**

Once again, *Zubulake IV* has a few suggestions. While recognizing that litigants are free to choose the method, *Zubulake IV* suggests that litigants might retain “all then-existing back up tapes for the relevant personnel” and catalogue all later created documents in a separate electronic file. The court suggests that, in addition, a “mirror-image” of the company’s computer system be taken at the time the duty to preserve attaches. *Zubulake IV*, 220 F.R.D. at 218.

**F. DOES A “LITIGATION HOLD” APPLY TO INACCESSIBLE BACK-UP TAPES (THOSE MAINTAINED FOR DISASTER RECOVERY)?**

The 2006 amendments to Federal Rule 34 clarify that “discovery of electronically stored information stands on equal footing with discovery of paper documents.” See Advisory Committee Note on 2006 Amendments. Consequently, without a qualifying reason, a party is no more entitled to access to an opponent’s electronic information storage systems than to the opponent’s warehouses storing paper documents. *Palgut v. City of Colo. Springs*, 2007 WL 4277564 (D. Colo. 2007) (holding that the “trigger date” by which defendant had a duty to preserve information was upon receipt of a litigation hold letter from plaintiff’s counsel, as opposed to a later date on which the initial complaint was served). However, if these electronic storage systems are actively used for information retrieval, they should be preserved pursuant to a “litigation hold” or at least a “reasonably accessible” analysis. See F.R.Civ.P. 26(b)(2)(B) (“A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.”); *Zubulake IV*, 220 F.R.D. at 218.

**G. WHAT IS COUNSEL’S DUTY?**

*Zubulake V* instructs that a “litigation hold” is only the beginning. Counsel has a duty to “oversee compliance with the litigation hold.” And counsel has the responsibility to monitor the client’s efforts to retain and produce relevant documents. *Zubulake V*, 229 F.R.D. at 431.

**H. COUNSEL’S “TO DO” LIST**

The following is an additional, non-exhaustive list of suggestions derived from the *Zubulake* decisions:

- Develop a protocol for preservation, collection, and production of ESI.
- Respond promptly to document hold letters from the opposing party.
- Meet on a continuing basis with relevant information technology personnel.
- Become fully familiar with the company’s document retention policies and data retention system.
- Have the technology personnel explain the system-wide back-up procedures and actual implementation of the company’s recycling policy.

- Communicate with the “key players” in the litigation to determine how they store information. This means interviewing each key person.
- Document and follow up on your communications to these technology personnel and key players.
- Independently run counsel’s own “key word search” and then preserve a copy of each “hit” from the search. *Zubulake IV* recommends that counsel be creative, particularly where the size of the company or scope of the lawsuit makes it infeasible to talk to every key player.
- Ask yourself as counsel: “Am I taking affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched?”
- Retain copies of all data obtained and all new data generated.
- Resend the initial litigation hold instructions periodically to remind key players that they have a responsibility to preserve and that that duty is still in place.
- Be sure that all electronic data and back-up media are in counsel’s possession or otherwise safeguarded to avoid possible destruction by recycling of back-up tapes.