

*What's
Reasonable:
Application of the
New Federal
Rules and State
Rules on ESI to
the Discovery
Process and the
Impact on
Employees,
Employers, In-
house and Outside
Counsel*

November 9, 2007

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

I. INTRODUCTION

A. THE EXPLOSION OF ELECTRONIC EVIDENCE

Technological advancements have exponentially increased the universe of discoverable electronic material, changing the manner in which we must think about evidence.

- Over 80 % of all corporate data is created and stored electronically, and most of that data is never translated into hard copy form.
- A single computer tape or small disk drive can hold the equivalent of millions of printed pages.
- In 1998, there were approximately 47 million e-mail users in the United States. In 2003, it was projected that there would be 105 million e-mail users in the U.S. who would send over 1.5 billion e-mail messages per day, or approximately 547.5 billion e-mail messages per year.
- A 2003 Cohasset Associates survey of more than 2,200 records management professionals revealed that only 59% of the respondents stated that electronic records were included in their organization's current records management program, and that this number had not changed significantly in the past four years. Only 54% of those surveyed reported that their organization had a discovery request response plan, and 65% reported that their organization's system for records hold orders did not include electronic records. The complete survey is available at <http://www.merresource.com>.

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 amended rules acknowledge 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 begin to 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 should 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 amendments to the Federal Rules of Civil Procedure is the provision for 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’s note. Amended Rule 37(f) will provide a safe harbor against the sanctions provided for 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 could include “a party’s intervention to modify or suspend certain features of the routine operation to prevent the loss of information, if that information is subject to the 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 note suggests that good faith might require a party “to prevent the loss on sources that the party believes are not reasonably accessible.” 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.” *Id.* Finally, if a judge determines that “exceptional circumstances” exist, he may impose sanctions under Amended Rule 37 for data that is lost because of a system’s routine operation even if that operation was in good faith.

Information That Is Not Reasonably Accessible

Amended 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.” Amended Rule 26(b)(2)(B) advisory committee’s 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.” *Id.* Though the Amended Rule and its advisory committee’s note do not define information “not reasonably accessible,” examples of such information may include backup 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 specifies 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

Amended 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 Amended 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 Amended Rule will also allow 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 Amended 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 by above, Amended 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 Amended Rule anticipates that such an agreement will save both parties time and expense by allowing parties to produce discoverable information more quickly, while allowing the parties to later claim privilege or work product protection on materials they have already produced.

Electronic Document Preservation

Though the rules do not discuss the nature of a party’s preservation responsibility, Amended 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 changing and because the costs to compile and preserve this information can be significant. Thus, the advisory committee note suggests 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 seek to ensure a uniform approach to the discovery of electronic data. For instance, Amended Rule 33(d), regarding the production of business records in response to an interrogatory, will specifically include the production of electronic business records. The advisory committee note states, however, that in order to meet the requirements of the Amended Rule,

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, will specifically recognize “electronically stored information” as a distinct category of data, separate from “documents.” Amended Rule 34 will also allow 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, Amended Rule 26(f)(3) will require 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.” Amended Rule 34(b)(ii).

Companies Should Take Immediate Action

Companies and corporate counsel should be aware of the amended rules and take appropriate measures. For instance, now, more than ever, it is important to have clear and open communication between the IT department and the legal department. At a minimum, corporate counsel should regularly meet with IT personnel to discuss the company’s information technology systems so that they understand the nature and scope of the company’s electronic data, the systems supporting the data, the policies regarding storage of the data, and the capabilities of the system in terms of preserving certain data on a moment’s notice. In addition, it is important that document retention policies recognize the distinct nature of electronic data, as do the amendments to the Federal Rules. Corporate counsel should discuss the company’s document retention policies and any preservation obligations with the IT department to ensure knowledgeable compliance. Companies must also be aware that these rules, particularly those governing the safe harbor for data destroyed in the routine operation of computer systems and the rules pertaining to inaccessible data, may lead to the deposition of or consultation with the company’s IT personnel in order to understand the nature of potentially responsive data and the capabilities of a system. Ultimately, a corporate counsel’s familiarity with the requirements of these rules and their company’s electronic data management policies and systems can lead to greater ease and less expense at the outset of litigation.

C. A LACK OF GUIDANCE

Until the recent amendments to the Federal Rules, judges and attorneys have 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 have 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 have been developing new rules on an ad hoc, often highly fact-specific basis. Consequently, at present, there exists no clear rules sufficient to address the complexity of issues that even the most simple of discovery requests can raise in relation to electronic evidence.

D. DEVELOPING STANDARDS

In a garden-variety sex discrimination case brought against UBS Warburg LLC, U.S. District Judge Shira Scheindlin has written a series of thoughtful decisions addressing the electronic evidence retention and search obligations of a defendant in civil litigation. Although the *Zubulake* decisions are not binding on other courts, and some courts have expressly declined to follow Judge Scheindlin's directives, the decisions are nevertheless instructive. 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*"). In *Zubulake IV*, Judge Scheindlin held:

"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 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 client and counsel's obligations with regard to 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.¹ . . . 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.*

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 are also 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 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*,

¹ 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.

57 P.3d 255 (Wash. 2002) (noting that “[a]lthough some email services may offer the possibility of ‘shredding’ an email message, arguably the equivalent of actually deleting it, the email 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:

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

It is metadata that provides a blueprint of a backdated document or reveals 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; or
- 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 continue to reside on the hard drive until they are 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. WHEN IS PRESERVATION AND/OR PRODUCTION OF THE DATA COMPRISING THE DIGITAL TRAIL REQUIRED?

“A discovery request aimed at the production of records retained in some electronic form is no different in principle from a request for documents contained in any office file cabinet.... To permit a corporation... to reap the business benefits of such [computer] technology and simultaneously use that technology as a shield in litigation would lead to incongruous and unfair results.”

Linnen v. A.H. Robbins Co., 1999 WL 462015 (Mass. Super. June 16, 1999).

"...[T]he duty to preserve has got to be broader than your duty to produce....If this stuff is gone, I can't rule.... In most cases, the producing parties in the kind of cases where this matters are fairly big companies. To preserve data to me is a cost of doing business. You always had to preserve data."

Judge Scheindlin, LEGAL NEWS, Vol. 72, No. 24, Jan. 26, 2004.

As the following discussion demonstrates, some courts have embraced the sentiments expressed in the above passage, and demonstrated an inclination to require litigants to preserve and produce data in the form most useful to and, therefore, manipulable by the opposing side. Given the volume of data generally retained in electronic form, however, such an approach can be problematic if followed without consideration of the considerable burdens it may impose upon the producing party.

A. CASES IN WHICH COURTS ORDERED PRESERVATION

1. Backup Tapes

- *Zhou v. Pittsburgh State University*, 2003 WL 1905988 (D. Kan. Feb. 5, 2003) (holding in employment discrimination case 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 backup 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 backup 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. Replicant / Embedded / Residual (Deleted) Data

- *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 as 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.”)

B. CASES IN WHICH COURTS ORDERED PRODUCTION

1. Backup Tapes

- *Kaufman v. Kinko's Inc.*, 2002 WL 32123851, at *2 (Del.Ch., Apr. 16, 2002) (ordering production of e-mails retrievable from defendant's backup 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, backup tapes created after notice of litigation; to provide plaintiff with access to a requested hard drive; and to produce backup 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 backup file of defendant's laptop computer, and a backup file of any personal computer hard drive to which defendant had access.)

2. Replicant / Embedded Data

- *Giardina v. Lockheed Martin Corp.*, 2003 WL 1338826 (E.D. La. Mar. 14, 2003) (ordering production, in an employment discrimination suit, 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

- *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. Super. 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 in trademark case.)
- *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

- *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: The eight factors are: (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 backup tapes.)
- *Toshiba America Electronic Components, Inc. v. Superior Court*, 124 Cal. App. 4th 762 (Cal. App. 2004) (the court concludes 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 exercise discretion on the reasonableness of expense shifted).

C. CASES IN WHICH COURTS REFUSED TO COMPEL PRESERVATION OR PRODUCTION

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

1. Preservation

- *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

- *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, in an employment discrimination suit, of electronic information on computer tape where all data was 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.”)

D. 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 backup 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

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.

- *Zubulake v. UBS Warburg LLC*, 2004 WL 1620866 (S.D.N.Y. 2004): (granting adverse inference jury instruction on content of deleted emails, and ordering defendant to pay for the re-depositions of relevant personnel, the restoration and production of backup tapes, and the “reasonable expenses, including attorney’s fees,” incurred by plaintiff. Jury subsequently reached \$19MM verdict based on adverse inferences.)
- *Coleman (Parent) Holdings Inc. v. Morgan Stanley, Inc.*, 2005 WL 674885 (Fla.Cir.Ct. 2005) (Court grants “death knell” adverse inference instruction for failure to preserve and search backup tapes.)
- *United States v. Philip Morris USA Inc.*, 327 F.Supp.2d 21 (D.D.C. 2004) (Court ordered the defendants to pay costs relating to the spoliation as well as \$2,750,000 in monetary sanctions for failing to stop routine email destruction post-preservation order.)
- *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.)

- *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 has asserted copyright infringement claims, and granting plaintiff the right to file appropriate motions for sanctions as the case develops.)
- *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.)
- 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 backup tapes)
- *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.)
- *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 the e-mail of the five key employees that the company itself had identified as having relevant data.)

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 EMPLOYER PRESERVE ELECTRONIC DATA?

Duty to preserve may arise even before an EEOC complaint is filed. It arises when the employer 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 v. UBS Warburg LLC, 220 F.R.D. 212, 216-217 (S.D.N.Y. 2003)
(*Zubulake IV*)

B. WHAT MUST BE PRESERVED?

The employer 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 in the initial 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). Therefore, it appears that the employer (and his counsel) must get into the head of the employee and ask what would the employee reasonably, likely be requesting?

C. DETERMINE WHAT DOCUMENTS ARE ACCESSIBLE OR INACCESSIBLE.

Whether demanding electronic data in discovery or objecting to it as undue burdensome or expensive, the accessibility or inaccessibility is the primary question. The court in *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309, 319-20 (S.D.N.Y. 2003) (*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) backup tapes and (2) erased, fragmented or damaged data.

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 “key players” in the case. *Zubulake IV*, 220 F.R.D. at 217-218.

E. WHAT MUST BE RETAINED?

In *Zubulake IV*, again we find guidance that the employer “must retain all relevant documents... in existence at the time the duty to preserve attaches in any relevant documents created thereafter.” *Zubulake IV*, 220 F.R.D. at 217.

F. 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 to catalogue all later created documents in a separate electronic file. The court suggests that, in addition, a “mirror-image” of the employer’s computer system be taken at the time the duty to preserve attaches. *Zubulake IV*, 220 F.R.D. at 218.

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

No. However, if they are actively used for information retrievable then they likely would be. *Zubulake IV*, 220 F.R.D. at 218.

H. WHAT IS THE EMPLOYER’S COUNSEL’S DUTY?

Zubulake V instructs that “litigation hold” is only the beginning. Counsel has a duty to “over see compliance with the litigation hold.” Counsel has the responsibility to monitor the client’s efforts to retain and produce relevant documents. *Zubulake v. URB Warburg, LLC*, 229 F.R.D. 422, 431 (S.D.N.Y. 2004) (*Zubulake V*).

I. COUNSEL'S "TO DO" LIST

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

- Respond promptly to document hold letters from the employee.
- Meet on a continuing basis with relevant information technology personnel.
- Become fully familiar with the employer's document retention policies and data retention system ("architecture").
- Have the technology personnel explain the system-wide back-up procedures and actual implementation of the employer's recycling policy.
- Communicate with the "key players" in the litigation to determine how they store information.
- This means interviewing each key person. (But see subparagraph 9. viii below.)
- Document and follow-up 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 not feasible 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?"
- Personally retain copies of all data obtained and all new data generated.
- Resend the initial litigation hold instructions periodically to remind key players of the responsibility to preserve and that duty is still in place.
- Be sure that all electronic data and back-up media are in your possession or otherwise safeguarded to avoid possible destruction for recycling of back-up tapes counsel should do it.
- Develop a protocol for preservation of documents.