ESI: ELECTRONICALLY STORED INFORMATION THE NEW FEDERAL RULES REGARDING PRESERVING AND PRODUCING ESI

By:
Christopher S. Hickey

INTRODUCTION

From the first electrical signals tapped out by telegraphs in the mid-19th Century to the development and use of personal computers ("PC") in the late 1970s, the production of records during litigation consisted primarily of paper documents. Since those early PCs, electronic media products have grown exponentially in both their numbers and power. The PCs, laptops, personal digital assistants (PDAs), etc. that occupy office desks, homes and that are holstered to employees' hips are pumping a never ending flow of electronic data into intranets, networks and the Internet. They have created what is currently a 91,000 terabyte[1] Leviathan of invisible electronic data.

As the use of electronic media exploded in the workplace over the last quarter-century, so has the volume of electronically stored information ("ESI"). The shift from paper to electronic records has been staggering. In today's business world, more than 90 percent of all information is created and retained in an electronic format. Estimates are that 70 percent of those electronic files are never even converted to hard copies. Large companies now measure their ESI in terabytes. Consider just the volume of e-mails generated each year: an average employee writes or receives about 50 e-mails per day. That adds up to over 10 million e-mails each year for a company with just a 1000 employees. For the larger multinational companies, the number reaches the billions.

---

[1] One terabyte is equal to about 500 million typewritten pages. For comparison, the entire Library of Congress would be approximately 11 terabytes.

While these technological advances have generally resulted in a more efficient, connected, and productive working environment, they present significant challenges in litigation discovery. Simply put, the discovery of computer-based information costs more, takes more time and creates more headaches than conventional, paper-based discovery.

Beginning in 2000, a process was initiated to bring the Federal Rules of Civil Procedure ("Rules") into the 21st Century. After six years of law journals, articles and public hearings on the subject of ESI discovery, rule changes were approved by the United States Supreme Court and became effective on December 1, 2006. The changes were implemented in an attempt to alleviate the burden, expense and uncertainty that resulted from the application of traditional discovery principles to ESI.

Electronic discovery has become the toughest litigation-related hurdle facing litigants today. As such, it is imperative that attorneys and corporations thoroughly understand their responsibilities under the amended Rules. A company that takes the time to prepare and implement the necessary changes to comply with the new Rules, will be able to more efficiently produce ESI and avoid the potentially devastating sanctions that some courts have issued in recent years.

WHY IS ESI DIFFERENT?

ESI's distinct characteristics prevent it from being assimilated into traditional discovery rules. First, ESI is dynamic. It can be altered or destroyed by the ordinary operation of a computer, frequently without the operator's knowledge or direction. Second, ESI is, simultaneously, persistent and may be stored in a variety of different forms and locations (including servers, backup tapes, desktops, laptops, PDAs, home computers, etc.). Even when an operator intends for a document to be deleted, it likely is not. The file remains on the operator's computer hard drive, the company's back-up drives or in a number of other

locations if the operator at any time shared that document with other computer users. This unique feature of electronic discovery gives rise to issues regarding whether that retrievable information is still discoverable and if so, under what circumstances and who must bear the burden of the expense required to search for, and retrieve, the file. Third, as already explained, the volume of ESI discoverable information has increased dramatically in recent years. Due to these distinct characteristics of ESI, application of the old rules proved inadequate to provide the necessary guidance to both courts and litigants. Change was necessary.

The Judicial Treatment of ESI Discovery Disputes

The first attempts to address the unique problems associated with ESI were made by the courts as early as 1986.[2] The most significant examination to date was provided by Judge Shira A. Scheindlin in her landmark decisions in *Zubulake v. UBS Warburg.*[3] Judge Scheindlin's opinions provided detailed guidance—much of which is mirrored by the December 2006 Rule changes—with regard to defining "accessible" vs. "inaccessible" data, the duty and responsibility of the parties and their counsel to locate, preserve and produce ESI and the penalties for failing to adequately respond to ESI discovery requests.

The *Zubulake* case involved plaintiff, Laura Zubulake, a former equities trader. Ms. Zubulake sued her former employer for gender discrimination, failure to promote, and retaliation under applicable federal, state, and city law. During discovery, she asked for the production of "[a]ll documents concerning any communication by or between UBS employees concerning Plaintiff." When UBS produced only about 100 e-mails, Zubulake argued that there must be more e-mails stored on UBS' back-up

---

2 *See Row Entm't, Inc. v. United States*, 50 F. Supp. 1003 (1986) (the translation of electronic data should be in a form useable by the discovering party).

3 A group of five separate decisions known as *Zubulake I-V*.

tapes. UBS objected to producing the back-up tapes, arguing that it would cost approximately $300,000 to restore and review this data.

In *Zubulake I*,[4] Judge Scheindlin drew a distinction between "accessible" and "inaccessible" data. She did so in the context of deciding whether to shift the cost of production to the requesting party, but the accessible/inaccessible distinction adopted by the 2006 Rule changes was not only in the context of cost-shifting but also with regard to the types of ESI that need to be searched for and produced by a party.

Judge Scheindlin determined in *Zubulake I* that cost-shifting should be considered when the production of electronic information is unduly burdensome or unduly expensive. This analysis "turns on whether the information is kept in an accessible or inaccessible format." The court laid out the five categories of storage media, from most to least accessible: (1) active, online data; (2) near-line data; (3) offline storage/ archives; (4) backup tapes; and (5) erased, fragmented or damaged data. The court found that data in the first three categories is "accessible" because the data in that type of storage media is in a "readily useable format" and "does not need to be restored or otherwise manipulated to be usable." Data stored on the last two categories are "inaccessible" because the information needs to be restored or reconstructed. According to Judge Scheindlin, "it would be wholly inappropriate to consider cost shifting" for "accessible" information but it would be appropriate for "inaccessible" information.

In *Zubulake V*,[5] Judge Scheindlin provided a detailed guideline for corporate in-house and outside counsel to follow to ensure that the corporation fulfills its duty to locate, preserve and produce relevant ESI. While the guideline was not expressly mentioned by the new Rules changes, given the wide spread

---

4 217 F.R.D. 309, 318-320 (S.D.N.Y. 2003).

5 229 F.R.D. 422 (S.D.N.Y. 2004).

acceptance and national acclaim of the *Zubulake* opinions, corporations and their counsel would do well to study and adopt Judge Scheindlin's guide:

(1) A "litigation hold" must be issued (and routine document retention/destruction policies suspended) whenever litigation is reasonably anticipated; this will include, at a minimum, instructions to produce all active electronic files and identify, retain and store in a safe place all back-up media; counsel must also periodically re-issue the litigation hold notice so that employees maintain their awareness of it;

(2) In-house and/or outside counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched; it is not sufficient to simply notify all employees of a litigation hold and expect that the employees will then identify, retain and produce all relevant information;

(3) Counsel must become fully familiar with the company's document retention policies and data retention architecture; this will involve speaking with IT personnel;

(4) Counsel must communicate with "key players" in the litigation in order to understand how they stored information (i.e., hard copy, electronic or both) and to determine whether all potential sources of information have been searched.

Lastly, in *Zubulake V*, Judge Scheindlin demonstrated the severe penalties that can result from a less than energetic effort to locate, preserve and produce ESI evidence. She imposed sanctions against UBS for destroying a number of potentially relevant e-mail messages and the tardy production of other e-mails. In addition to monetary sanctions related to the cost of re-deposing certain individuals due to the tardy production of certain e-mails, Judge Scheindlin ruled that the jury be given an instruction that they are permitted to infer that the lost evidence would have been unfavorable to UBS. The jury found in favor of the plaintiff and

ordered UBS to pay $9.1 million in compensatory damages and $20.1 million in punitive damages.[6]

The December 2006 Changes to the Federal Rules

Spurred by the *Zubulake* decisions, the American Bar Association revised and updated its standards regarding document preservation and production to address practical aspects of electronic discovery not previously addressed by the rules. The ABA stated the changes were needed in order to assist companies and counsel in (1) completing effective discovery and (2) avoiding spoliation problems. In 2004, the Civil Rules Advisory Committee held meetings to address ESI issues. Out of these discussions came a number of proposed amendments. These revisions were ultimately approved by the U.S. Supreme Court and became effective on December 1, 2006.

The December 2006 amendments to the FRCP address a number of the problems unique to ESI regarding the burden and cost of preserving and producing certain data, the format in which ESI should be produced and the penalties for non-compliance. Primarily addressed were Rule 26 (initial disclosures and scope of discovery), Rule 34 (format of ESI production), and Rule 37 (sanctions). Although it is still unclear exactly how courts will interpret and apply the amended rules, the changes have sent a

---

[6] Other recent cases have also levied heavy sanctions for ESI production shortcomings. *See United States v. Phillip Morris*, 327 F.Supp.2d 21 (D.C. 2004) (The court found Phillip Morris' failure to preserve e-mails in violation of the court's preservation Order. In calculating a $2.75 million sanction amount, the court fined each corporate manager and/or officer (11 total) who failed to comply with the company's "print and retain" policy $250,000 each.) and *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, No. 03-5045, slip op. at 16 (15th Jud. Cir. March 23, 2005)(The court reversed the burden of proof on the aiding and abetting and conspiracy claim and included a statement of evidence of [Morgan Stanley's] efforts to hide its e-mails to be read to the jury, as relevant to both its consciousness of guilt and the appropriateness of punitive damages.)

strong message to litigants that e-discovery issues are not to be ignored. As such, competent legal representation now requires a thorough understanding of clients' electronic data architecture.

1. Litigants Need to Preserve All ESI and Produce *Accessible* ESI

Rule 26 was amended to specifically address the rising cost of ESI discovery requests, especially difficult to retrieve ESI requiring the assistance of an information technology specialist. The amendments adopt a new standard that embraces the distinction introduced in the *Zubulake* opinions, between "accessible" and "inaccessible" data.

a. All ESI needs to be preserved

The amended Rules require that all potentially relevant ESI be preserved once litigation is reasonably anticipated—as is the case with any other type of potential evidence.[7] This includes both *accessible* and *inaccessible* ESI and might even include electronic data on employees' home computers, personal flash-drives, cell phones, PDAs, etc. Once the parties identify all potential sources of ESI, it may be reasonable for parties to continue their normal electronic data destruction policy for all inaccessible data—even if that data has potentially relevant material.[8] However, that issue is to be handled by the courts on a case-by-case basis. A party to litigation should maintain all electronic data until the court and/or parties agree otherwise.

b. Parties must meet and confer regarding ESI discovery

After all ESI with potentially relevant information has been secured from destruction, litigants must next meet and confer

---

7 Rule 26(b)(2).

8 *See* Advisory Committee Notes to Rule 26(b)(2).

to discuss potential discovery disputes. The amended Rule 26(f) now expressly requires that the parties include in their meet and confer conference "any issues relating to the disclosure or discovery of electronically stored information, including the form or forms in which it should be produced."[9] The "issues" that will likely need to be discussed in every initial Rule 26(f) conference are (1) the volume of ESI; (2) how it is being stored; (3) how each party intends to search for potentially relevant ESI; (4) the form in which electronic discovery will be produced; and (5) data preservation.

The Rule 26(f) changes are significant because they force counsel to confront the electronic discovery issues very early in a case. Rule 26(f) meet and confer must occur no later than 21 days before the scheduled initial status conference. Thus, counsel representing corporate parties need to hit the ground running when it comes to ESI. Corporate and litigation counsel need to meet with key IT department individuals soon after a complaint is served in order to gain an understanding of the company's ESI architecture including the volume, manner in which it is stored, what data is accessible and inaccessible and what outside vendors, if any, play a role in the company's ESI system. An early understanding of the ESI structure will help to reduce the number of later discovery problems and discovery costs.

c. Initial disclosures must include a description of *all* ESI

Within 14 days of the Rule 26(f) conference discussed above (unless a different time is set by stipulation or court order), the parties are required by the federal rules to provide Initial Disclosures to opposing counsel. Initial Disclosures include, among other items, a list of all people and documents likely to have discoverable information. Litigants must now include in its Initial

---

[9] Rule 26(f).

Disclosures "a copy of, or a description by category and location of, all electronically stored information" that "the disclosing party may use to support its claims or defenses".[10]

As with the change to Rule 26(f), the addition of ESI to the requirements of Initial Disclosures necessitates an early understanding of a client's technology and storage architecture. If counsel is unprepared or unfamiliar with their clients' systems, the time allotted for compliance may be insufficient to identify potentially helpful ESI materials.

d. Parties must only produce *accessible* ESI

From the corporate perspective, the most troubling aspect of the early court rulings on ESI discovery was the somewhat cavalier attitude courts had with regard to the time, effort and money it takes to find, reconstruct, review and produce electronic data stored on hard-to-access back-up tapes and other storage media. In some cases, complying with discovery orders required the reconstruction and production of millions of electronic files—most or all of which were useless to the litigation—at costs to the company of hundreds of thousands of dollars. The new Rule 26(b) provides a much needed salve.

The amended Rule 26(b) significantly reduces the initial breadth of ESI discovery and halts, at least temporarily, the potential deluge of ESI a company might otherwise be forced to find and produce. Under the new Rule, "[a] party need not provide electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost."[11] Instead, those ESI sources which the responding party is neither searching nor producing must simply be identified by category or type. The identification needs to be of sufficient detail "to enable the requesting party to evaluate the burdens and costs of

---

[10] Rule 26(a)(1)(B).
[11] Rule 26(b)(2)(B).

providing the discovery and the likelihood of finding responsive information."[12] Once properly identified, a court may only order discovery of inaccessible data upon a finding of "good cause".[13]

The amended Rules essentially create a two-tiered system regarding the production of ESI. Electronically stored information that is easy to access should be produced, as requested. However, data that is difficult to access, even though potentially responsive to the discovery request, may be withheld on the basis that it is too burdensome and expensive to access or retrieve.

e. Seeking the production of "inaccessible" data

As discussed above, a party can be required to produce inaccessible electronic data by court order after a showing of good cause by the requesting party.[14] In determining whether good cause has been shown, the court must balance the costs and potential benefits of such discovery. Appropriate consideration may include: (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessible sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information; (5) predictions as to the importance and usefulness of further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources.[15] Even if good cause is shown, the court maintains the authority to set conditions on discovery such as "limits on the amount, type, or sources of information required to be accessed and produced."[16]

In addition to *weighing* the costs as part of its "good cause" analysis, a court can also *shift* the cost of production to the

---

12 Advisory Committee Notes, Rule 26.
13 Rule 26(b)(2)(B).
14 Id.
15 Advisory Committee Notes to Rule 26(b)(2).
16 *Id.*

requesting party. Traditionally, it has been the presumption that the responding party bears the expense of complying with discovery requests. Such compliance, however, can be extremely costly with regard to inaccessible ESI. The revisions to Rule 26 address this concern and appear to adopt the cost-shifting principle suggested by Judge Scheindlin in *Zubulake I* (i.e., cost-shifting may be appropriate in the case of producing "inaccessible" data). The Advisory Committee Notes to Rule 26 state that "[a] requesting party's willingness to share or bear the access costs may be weighed by the court in determining whether there is good cause [to produce inaccessible data]."

2. Format of ESI Production and the Concern Over *Metadata*

There are a number of formats in which ESI may be produced but the "Native File" is currently the most desirable from the perspective of the party making the request. "Native File" means in the electronic format of the application in which the ESI was created, viewed and/or modified (i.e., producing a Word document as a Word document). Although electronic files can be just as easily read as static images in either Tagged Image File Format (TIFF or .TIF files) or Portable Document Format (PDF), a Native File will provide opposing counsel with all the embedded information that is not ordinarily viewable or printable from the application that generated, edited or modified the Native File. This embedded information is known as "metadata" and it is a potential bonanza of information which may allow the document viewer to see all prior edits to the document, when the file was created, who created it and, in some cases, who has viewed the electronic file and when. The production of metadata has been, and is being, hotly contested in the courts.

The December 2006 amendments to the Rules have added fuel to the debate. While metadata is not expressly addressed by any of the Rule changes, the Advisory Committee Notes suggest that whether metadata "should be produced may be among the topics discussed in the Rule 26(f) conference." In

addition, the new Rule 34 allows a requesting party to "specify the form or forms in which electronically stored information is to be produced", suggesting that the native file format may be specifically requested. Indeed, pursuant to the new Rule 34, even if a document discovery request for ESI does not explicitly address the format of production, the responding party is required to produce electronic files in either the form "ordinarily maintained or in a format that is reasonably useable."[17] While an electronic file can be easily produced in a manner that both maintains its usability but removes all metadata, the Advisory Committee Notes to Rule 34(b) include the following:

> If the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature.[18]

The ability to search by electronic means usually necessitates the use of the file's metadata. Indeed, Microsoft Excel files will not even operate without its associated metadata.

It is unknown, at the moment, how the 2006 amendments will impact the debate concerning the production of metadata. However, prior to the 2006 Rule amendments, and continuing into 2007, the case law generally has not required the production of metadata absent a clear agreement by the parties or a court order based on "a demonstrated particularized need for the metadata."[19] Showing a "particularized need" entails not only showing the potential relevancy of the metadata but also demonstrating a

---

17 Rule 34(b).

18 Advisory Committee Notes to Rule 34(b).

19 *O'Bar v. Lowe's Home Centers, Inc.*, 2007 U.S. Dist. LEXIS 39205, *13; *see also Wyeth v. Impax Labs* (D. Del. 2006)("Emerging standards of electronic discovery appear to articulate a general presumption against metadata."); *Kentucky Speedway v. NASCAR* (E.D. Ky. 2006) ("A party should not be required to produce metadata absent a clear agreement or court order.").

favorable cost-benefit analysis. The courts' main concern with metadata is the substantial costs associated with reviewing "for the purposes of redacting non-discoverable information contained in such Meta-Data."[20] In most cases, the courts recognize that the relevancy of the metadata to any issue in the litigation is too remote to justify such time and effort. Just as with the production of inaccessible ESI, even if metadata is ordered produced, the production may be the subject of cost-shifting from the producing party to the requesting party.

The suggested protocol for the discovery of ESI created by the United States District Court for the District of Maryland and a 2007 North Carolina case have separated the metadata issue into three types of metadata: "substantive," "system" and "embedded data". Substantive metadata is defined as data that reflects the substantive changes made to the document by the user. System metadata is information automatically generated by a computer system such as author, date and time of creation, and the date of any modifications. Embedded data is the text, numbers, content, formulas, etc. that are directly imputed into a file and are necessary for the operation of that file. These authorities suggest that (1) Embedded data is discoverable and, in most cases, should be produced as a matter of course; (2) System metadata should be produced subject to cost-benefit analysis; and (3) Substantive metadata should only be produced subject to a cost-benefit analysis and potential redaction since it, of the three types of metadata, has the greatest potential for containing privileged information.

Finally, just because the metadata does not have to be produced initially, does not relieve the party from preserving this type of data. A court may, at any time, determine that the metadata of a particular document needs to be produced. Thus, as with all ESI, a litigant should never dispose of any potentially relevant ESI during an on-going lawsuit.

---

[20] *O'Bar*, at *16.

3. The Consequences of Failing to Fully Preserve or Produce ESI

In response to a number of courts imposing some rather harsh penalties on corporations who failed to produce certain requested ESI, the 2006 Rule changes include a limitation on the authority of courts to impose sanctions. The new Rule 37 states that "[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

This amendment to Rule 37 provides a "safe harbor" to litigants, particularly those parties with large volumes of ESI. However, "good-faith" involves the party's intervention to suspend the routine destruction of ESI. In *Zubulake*, discussed earlier, the defendant did issue a litigation hold letter. Unfortunately, one of UBS' major shortcomings was that it did not notify the IT department of the hold or follow-up with employees to ensure that items were not being destroyed. As a result, e-mails were lost. The new Rule 37, while a positive amendment to the Rules, also further highlights the absolute necessity in issuing a litigation hold letter as soon as litigation is reasonably anticipated and adhering to the guideline set forth in that case regarding the preservation of evidence.

MAKE THE 2006 AMENDMENTS YOUR FRIEND, NOT YOUR ENEMY

The 2006 amendments helped to reiterate, clarify, and expand upon many of the same developing principles emerging from recent case law and legal commentary. If adhered to, the new Rules have the potential to greatly reduce the burden and cost of "e-discovery" and, if ignored, could result in severe fines and/or sanctions. Businesses and their counsel should, therefore, adopt the following policies regarding ESI to assure conformance with the new Rules.

(1) Create or review the company's ESI retention/destruction policies. Destruction of electronic data is a necessary business function. What ESI should be permanently retained and which can be destroyed on a routine basis will be different for each company and should be discussed with counsel. However, companies must ensure that the policy is consistent, company-wide and based upon objective factors such as age of the ESI, end of a product line, etc. Avoid gaps in time (that is, where newer ESI pertaining to a particular subject are destroyed even though older files are still saved). Always eliminate electronic materials systematically.

(2) Those members of the legal team (both in-house and outside counsel) that will handle document preservation and production must become fully familiar with the company's electronic data retention architecture. At a minimum, this needs to include an understanding of what ESI materials are "accessible" and "inaccessible".

The emphasis in the new Rules is for early discussion and resolution of ESI discovery issues. Waiting until litigation commences may not leave sufficient time for counsel to adequately learn and understand the company's electronic data system. This could result in ESI materials not being properly preserved and/or produced (even those materials which may benefit the company) and, ultimately, unfavorable sanctions.

(3) Establish a "litigation hold" policy for ESI as soon as litigation is reasonably anticipated. This will include, at a minimum, cancellation of all routine ESI destruction until counsel can identify the areas of the company's ESI architecture which may contain relevant information. In addition, all back-up hardware needs to be identified, retained and stored in a safe place. There also must be a procedure for issuing and periodically re-issuing the litigation hold notice so that employees maintain their awareness of it. With regard to ESI, particular attention should be given to the company's IT department and any outside vendor that stores ESI for the company. In many cases, the back-up files that each

maintains may contain information inadvertently destroyed by employees at their individual workstations.

Throughout the litigation, in-house and/or outside counsel must take affirmative steps to monitor compliance with all company litigation hold orders and all court discovery orders so that all sources of discoverable ESI information are identified and searched. The steps taken to accomplish the litigation hold should also be documented so the company will be in a better position to address any challenges to its preservation policy.

The new Rule 37 offers a golden "safe harbor" opportunity but it can only be utilized if the company takes all necessary steps to avoid the accidental destruction of ESI.

CONCLUSION

The breadth of the impact of the 2006 Rule changes is still an unknown. What is known is that electronic files will continue to predominate in the workplace for the foreseeable future. As such, ESI discovery will continue to be a significant, if not the most significant, issue during discovery. While some of the new Rules inflict additional discovery burdens on litigants, at least in the early stages of litigation, the changes, as a whole, provide an opportunity for parties to reduce the overall burden and expense associated with ESI discovery. That opportunity, however, is conditioned on companies and their counsel understanding the company's electronic data architecture and taking appropriate proactive steps to ensure that ESI is preserved, identified and produced during litigation.