

## ELECTRONIC DISCOVERY FOR MARITIME LAWYERS

Jhnette Hassell, Ph.D. \*Jack Molisani Heidi P. Magid Caroline Hiatt  
Electronic Evidence Retrieval, LLC  
141 Robert E. Lee Blvd.  
Suite 108  
New Orleans, LA 70124  
(504) 483-0201  
JHassell@ElectronicEvidenceRetrieval.com

No matter what type of case you are handling, chances are there is information pertaining to the case stored in an electronically readable format, such as emails, word processing documents, and spreadsheets. Some estimates say that 99% of all new information developed in the U.S. is in electronic form.<sup>1</sup> The new (December 1, 2006) federal rules dramatically affect the preservation and production of such electronically stored information (ESI) and these rules will have a dramatic effect on how attorneys prepare for litigation and how businesses store and produce records and information.

E-discovery—it's not just for computer cases anymore.

### I. Overview of the New Federal Rules on e-Discovery

---

On December 1, 2006, new rules concerning discovery of ESI came into effect.

During the past three decades, courts have seen increasing numbers of cases in which evidence was found on computers. Under the new e-discovery rules, ESI now includes any information stored in *any* electronic device, including cell phones, PDAs, cameras, Blackberries™, voicemail systems, or even toll tag logs, hotel room keys, alarm systems, and “smart” chips. Where ESI on computers used to be limited to documents and emails, ESI now includes internet text messages, Internet browser histories and “cookies,” operating system event logs, and more.

The previous discovery rules did not address some of the fundamental and important characteristics of electronic evidence, so new rules were created to address the way electronic evidence is managed within the legal system, particularly how it is produced in discovery.

To meet their obligations under the new rules, attorneys need to be more intimately acquainted with their clients' data systems; you must know where and how information is stored, and understand your clients' policies for managing their ESI, if any. Even if your client is a “little guy” and does not have or use computers, you need to know the rules of the road so that you can hold opposing counsels to *their* obligations under the new rules.

We will address the following new and amended e-discovery rules (the “Rules”):

1. The requirement that parties and courts address e-discovery issues early in the

- case and in greater detail than before;
2. An expanded universe of what is discoverable and expanded role of the trial attorney;
  3. The requirement that attorneys be familiar with such technology as “metadata” and “data retention architecture”;
  4. A provision for *safe harbor* from sanctions if responsive ESI is deleted in the normal course of business (routine, good faith operation); and
  5. A requirement that an *ESI litigation hold* be enacted when litigation is known or should have been known.

## II. About Computer Forensics

---

In order to understand the broad implication of the new rules, it is necessary to know a few basics about computer forensics.<sup>2</sup>

### *What Is Computer Forensics?*

*Forensics* in general is “relating to or dealing with the application of scientific knowledge to legal problems.”<sup>3</sup> *Computer forensics* is, then, the application of scientific knowledge about computers and other electronic devices to legal matters.

### *Deleting Isn't Deleting!*

When a user “deletes” information from a computer, the information disappears from the user’s view but usually continues to exist on the computer until it is overwritten with new data. Deleted material (or portions of it) can continue to reside on the drive for many years.

Some files are deleted but continue to exist in their entirety. Such deleted files can be recovered by many over-the-counter tools. However, in other situations, deleted information may be segmented, and scattered across many places in the electronic media. In general, it takes an expert and sophisticated forensic tools to recover the latter. In *Plasse v. Tyco*, the plaintiff claimed that he was wrongfully terminated while the defendant argued that the termination was based on the plaintiff falsely claiming to have an MBA. The plaintiff asserted he never made such a claim. A forensic examination of the plaintiff’s computer revealed not only that there was a version of the plaintiff’s resume in which he claimed to have an MBA, but also that the plaintiff had deleted it after he had an obligation to preserve it. The court dismissed the complaint citing this and other actions as “extensive and egregious misconduct.”<sup>4</sup>

### *Can We Ever Really Delete Information?*

There will be times, such as when a computer is being decommissioned and perhaps donated to a charity, when people want to *totally* remove information from computer hard drives. There are numerous software applications that overwrite personal information such as temp files, cookies (from Internet access), and deleted files, and still others that completely “wipe” *all* data from a drive.

While such secure deletion tools have legitimate uses, litigants who use such tools in an attempt to destroy evidence have found little favor with the court as each of these tools leaves some trace of its use. For example, in *Communications Center, Inc. v. Hewitt*,<sup>5</sup> the defendant used Evidence Eliminator™<sup>6</sup> to erase files, claiming that he was trying to hide evidence of an extramarital affair and questionable website visits. The log kept by Evidence Eliminator showed that some of the overwritten documents were likely to contain responsive material. Based on this, the magistrate recommended default on those claims in the case related to the deleted material and he assessed the fees and costs associated with the motion for sanctions to the defendant.

#### *ESI Can Be Inadvertently Changed in the Routine Course of Business*

When a user starts a computer running most versions of Microsoft Windows™, the computer writes data to all drives of the computer as part of the startup procedure. So the simple act of starting the computer can change potential evidence.

Virus and “adware” scanning programs can alter and/or delete files. Such software often runs automatically, without the user specifically invoking them.

Email programs may screen incoming email and classify some email as “junk,” dangerous, or “spam” and automatically delete them. A corporate email system may routinely delete mail that is a given number of days old unless the recipient has filed it in some manner.

Most companies have routine backup procedures that destroy data. For example, there may be seven backup tapes that are used in sequence, one for each day of the week. At any one time, the organization has seven days worth of backup tapes. If a litigation hold is received on day nine, backups for days one and two can be lost.<sup>7</sup>

#### *What Is “Metadata” and Why Is It Important?*

Applications such as word processors, spreadsheet applications, and drawing programs store information *about* the files they create in addition to the document itself. Such information is called *metadata*.

Metadata can contain the history of the document, including who created, modified, printed, and/or saved it, as well as the printers it was printed on. In some cases, the metadata contains the previous changes made to a document. This information can be accessed using computer forensic techniques. For example, the authors have used metadata to demonstrate to the court that the defendants in cases have taken electronic copies of the plaintiffs’ technical material, such as manuals and designs, modified the material, and sold the material as their own.

Bob SmithXC:\My Documents\ Plans\Mod 500\Tech Manual.doc Bob Smith A:\Tech Manual
--

### *Example 1—Metadata*

Example 1 shows metadata from an actual case, although the names have been changed. It shows that the Tech Manual was moved from the employee's office computer to his home computer via a floppy disk.

### *What Is a Valid Forensic Image?*

As we have discussed, there is much information that operating systems track that is not available to a typical user. We have also pointed out that merely starting a computer system causes information to be written to every hard drive in the computer. How then is computer forensics possible?

The answer to this question is to create a *valid forensic image*—a bit-by-bit copy of the suspect drive. To do this without changing the data on the drive, forensic experts use “write blocking” devices between the suspect drive and the computer used to make the image. The write blockers intercept the write commands the operating system sends, thus preventing the drive from being altered.

### *What Is a Data Retention Architecture?*

The term “computer backup” usually refers to copies of files (documents, data files, and so on) that are created in case something happens to the original data. These backups play a central role in an organization's record retention policy. Some backup procedures are simple, such as an individual user copying a day's work onto another drive or computer. As organizations get larger, such simple procedures are inadequate for managing the large amount of data that must be backed up.

A typical retention architecture might use daily system backups that are made and kept on-site. At the end of each week, a weekly backup is made and stored in some off-site location. Similarly, monthly and annual backups are made and kept both on-site and at the off-site location. In addition, a copy of each annual backup is kept in some archival storage, such as a bank vault.

## III. The New e-Discovery Rules

---

Now that we have addressed some of the basics of computer forensics, let us look at how they apply to the new e-Discovery rules.

### *Early Notification of ESI (Rule 26(a)(1)(B))*

In the past, computer files containing potential evidence were often not known or disclosed until late in the discovery period. Rule 26 has been amended to direct parties to include a discussion *during the scheduling conference* of whether ESI will be involved in the case. In effect, Rule 26(a)(1)(B) mandates a deadline by which attorneys must

discuss what ESI is related to their case. The Rule is explicit:

the parties **must** . . . at least 21 days before a scheduling conference . . . confer **to discuss**:

...a party must, without awaiting a discovery request, provide to other parties: a copy of, or a description by category and location of, all documents, *electronically stored information* ...that the disclosing party may use in support of its claims or defenses.<sup>8</sup>

In this amended Rule, and throughout the Rules, the phrase “data compilations” was replaced by “electronically stored information.” This change broadens the scope of possible discovery to include all information stored on computers and other electronic media. ESI may be found and subject to discovery on all the following devices:

Sound recordings	Text messages	Cell phones
Photographs	GPS locators	Flash media
SD	Cameras	Toll tags
Voicemail	iPods	MP3 players
Voicemail servers	Internet logs	Internet “cookies”
Blackberries	Smart phones	Car computer

*Preserving Discoverable ESI and the Consequences of Failing to Do So (Rule 26(f)) and (Rule 37(f))*

Federal Rule 26(t) states in relevant part that “In conferring the parties must . . . *discuss any issues related to preserving discoverable information.*”<sup>9</sup>

There are many ways in which ESI can be lost unintentionally. As we discussed earlier, companies rotate and reuse their backup tapes, and they may delete email once it reaches a certain age. Databases are modified as new information is added or changed. Most applications, such as Microsoft Word and Excel, keep a list of recently used files, the so-called Most Recently Used (MRU) list. When an MRU list reaches its maximum, the oldest link is removed from the list and a new one is added.

Under the new section of Rule 37, parties may not be sanctioned for the loss of electronically stored information if it is due to “routine” business practice and if they acted in “good faith.” In other words, the new Rules provide a *safe harbor* with respect to sanctions if discoverable ESI was lost due to routine operations of the responding parties’ information systems.

The preservation of ESI has special challenges due to the volatile nature of data stored on electronic media. Since it is easy to alter ESI, the best strategy for preserving ESI is to stop using the devices when a litigation hold is received, minimizing the risk that possible evidence is overwritten. The problem with this approach, of course, is that it takes all suspect machines out of use, potentially stopping a business dead in its tracks and certainly giving opposing counsel an understandable argument that responding is unreasonable burdensome.

Another approach is to temporarily remove relevant machines from use until the data can be properly preserved. When servers and hundreds of machines are involved, this can significantly hinder a company's ability to conduct business, but at least it complies with the litigation hold.

Our recommendation is to create a valid forensic image of the relevant drives. The advantage to securing a valid forensic image of the relevant drives is that a business can return to full operation quickly. Fortunately there are now tools that can acquire images of servers without interrupting the network's operation. Given the size of some of the penalties that have been meted out, the personnel costs of retrieving and reviewing data responsive to discovery requests and interrogatories, and the costs associated with business interruption, an investment in a valid forensic image may well make good business sense.

When the opposition is a large organization, its counsel will no doubt argue that making such an image is unduly burdensome, too costly, will provide access to privileged information and work-product, and violate trade secret and copyrights.

In *Ameriwood Industries, Inc. v. Liberman*, the plaintiff alleged that former employees improperly used the plaintiff's company computers. The court held that there was good cause to *mirror-image* (i.e., make a valid forensic image) of the former employees' computers. The court reasoned that mirror-imaging was warranted because whether and how the defendants used certain electronic files was central to plaintiff's case.<sup>10</sup>

We recommend a particular solution to the inevitable opposition to creating an image. The requesting party retains an e-discovery or forensic expert who creates a valid forensic image and processes it for the search term and document types the requesting party designates. The findings are produced to the counsel for the *responding* party for review. The responding party redacts material as it deems privileged or otherwise objectionable.

#### IV. Routine Operation

---

As we have discussed, there are many ways ESI can be lost. For an organization to say that a particular loss is a result of routine operations requires that there *be* a "routine" operation, that is, a policy statement defining routine operations. Such *record retention and deletion policies* describe what materials are to be kept, how long and in what form they are kept, and when and how they will be disposed of. In this case, "record" includes all data kept in electronic devices as well as traditional paper records.

#### V. Good Faith

---

To operate in good faith, the opposing parties must be able to show that they have preserved the appropriate ESI. In *In re Old Banc One Shareholders Securities Litigation*, the court has taken notice of the need for such record retention and deletion plans.

The court concluded that Bank One should create a "comprehensive document retention

policy to ensure that relevant documents were retained and needed to disseminate that policy to its employees.”<sup>11</sup>

Failing the “good faith” test can lead to summary judgments, financial penalties, or a negative inference instruction to the jury. For example, a jury awarded \$1.45 billion against Morgan Stanley due to the court’s instruction to the jury that they consider the company’s discovery abuses.<sup>12</sup>

The second article of “good faith” is what the opposition does in the face of a litigation hold or knowledge of potential litigation. In developing a litigation hold policy, an organization should give serious consideration to creating a valid forensic image of the computers and other devices that may hold responsive material.

*The Form for Producing ESI (Rules 33 and 34(a))*

The changes to these two rules include ESI among the types of business records that are subject to discovery and subpoena. Due to the nature of ESI, the 34(a) amendment also adds sound recordings, images, cell phone records—*any* type of electronically stored information—to the types of data that may be called for in discovery.

Attorneys and their clients face some particular challenges when it comes to determining in what form e-discovery is to be produced. For example, ESI may be proprietary to a vendor. Does providing the ESI in its native form violate copyright agreements? The ESI may be a trade secret of the producing party. How does that party protect its trade secrets and copyrights? ESI may require specialized or proprietary hardware that the requester does not have. How does the requesting side access the ESI? The requesting side may not have the technical expertise needed to operate the opposing side’s software and/or hardware. How can the requesting side be able to inspect the ESI properly? As with the rules describing discovery of other business documents, the new rules anticipate that ESI will be produced in the form in which it is routinely kept and used. But, respondents to e-discovery requests may provide ESI in an alternate form that is “reasonably useful.”

For instance, if the requested ESI was created and saved in a common word processing program, the responding party *may not* save it in an engineering program that would make it more difficult or impossible for the requesting party to access during litigation. In one case in the authors’ practice, the opposing side first printed and then scanned its emails into the TIFF format, which is not searchable. This format prevented electronic searching for relevant names and required that each email be read individually. Such degradation of usability is prohibited under the 2006 amendments.

The Rules are explicit in one aspect of the form of ESI: If the party producing the ESI can search it electronically, it must be presented to the requesting party in an electronically searchable form.

## VI. Ready for e-Discovery

---

The requirements of the pre-trial scheduling conference make it clear that opposing attorneys are going to have to address how they deal with cases involving e-discovery.

In *Zubulake*, the court addressed obligations of counsel.

The Court held that it was not enough for legal counsel to merely instruct a client to preserve email, but counsel must also take *affirmative steps* to ensure that evidence is preserved . . . more diligent action on the part of counsel would have mitigated some of the damage caused by UBS' deletion of emails.<sup>13</sup>

Aided by the *Zubulake* case, we offer a plan for dealing with opposing parties and their obligations with respect to e-discovery.

### *What Opposing Counsel Must Do*

In *Zubulake V*, the court lists three imperatives:

1. Issue a litigation hold at the outset of litigation or whenever it is anticipated;
2. Communicate directly with the key players in the litigation, i.e., those identified in the party's initial disclosure; and
3. Instruct all employees to produce electronic copies of their relevant active files.<sup>14</sup>

### *Preparing for the Pretrial Scheduling Conference*

There are differences in opinion among judges and jurisdictions in how the Rule 16 consultation must be carried out, but, as we have seen, the Rules are explicit in requiring opposing attorneys to be knowledgeable concerning their client's ESI.

Consider developing a list of questions to guide your discussions with opposing counsel:

- Show me the list of your client's ESI by location and contents.
- Have you issued a litigation hold to your client? If so, when did it go into effect? How are you monitoring your client's employees to insure compliance?
- Do you have a litigation hold plan? What are the procedures when there is a litigation hold?
- Can you assure that all employees follow all the policies and practices disclosed above? If so, how? If not, who does not and what does he/she do instead?
- What electronic applications does your client use? Include voice mail, voicemail servers, Blackberries, SmartPhones, flash media and so on.
- What metadata is available in each application your client uses?
- What are your client's backup procedures?

- Where are backup materials held? Who has access to them?
- Does your client have offsite backup storage? What form is it in?
- Are there indexes or other materials that identify what is on each backup item?
- Does your client still have all the hardware to read/access all the backup materials?
- What is the practice about individuals backing up their work as opposed to relying on the backups made by the IT department? If individuals make their own backups, where are they stored? How long are they kept? Who has access to them?
- Are employees allowed to take home laptop computers or external drives to use at home? If so, where is that material backed up? What is the policy about recycling the backup media they use?
- Are employees allowed to use their personal computers to access the office computer network?

Similar detailed questions can be asked about email, computer system administration, email servers, laptops, used equipment disposition, voicemail servers, scanners, fax machines, cell phones, and PDAs.

The amount of information the opposing counsel needs for preliminary discussions is extensive; your knowing about it may help lead to a quick settlement.

## VII. Getting Help

---

The American Bar Association has introduced the concept of an e-Discovery Liaison, of which the first author is one. Such experts:

- Provide techniques that can preserve data and provide chain of custody.
- Use sophisticated searching techniques that help identify relevant materials in a production, thereby reducing your time in reviewing discovery.
- Evaluate the oppositions' document retention policies.
- Teach attorneys, judges, and juries about ESI and its characteristics.
- Assist in developing protocols and procedures for attorneys who are involved in e-discovery.
- Easily determine records that are duplicates or "near duplicates", thereby reducing counsels' document review time.<sup>15</sup>

## VIII. Conclusion

---

Computer forensics has matured from a “seat-of-the-pants” art practiced by a few to a solid partner in the litigation process. As computer usage as a basic communication device has increased so has the likelihood that ESI may play an evidentiary role in litigation.

ESI as evidence requires different handling than traditional paper evidence in everything from practical matters, such as how to redact parts of a document, to procedural matters, such as avoiding spoliation of electronic evidence.

Trial attorneys are being drawn into e-discovery both by the changes in the Federal Rules of Civil Procedure and by the sheer volume of electronic evidence that arises in litigation. And, they must master concepts such as metadata and data retention architecture, concepts that change as new versions of operating systems and browsers are released. The good news is that there are excellent software tools and a cadre of well trained experts in computer forensics and e-discovery at the disposal of internal and trial counsel.

## Endnotes

---

\*The reader should note that the authors are not attorneys and we do not give legal advice. However, we are computer forensic investigators and e-discovery consultants and offer advice on the various forensic tools and techniques available to trial attorneys and their clients.

<sup>1</sup>Peter Lyman & Hal R. Varian, *How Much Information 2003?*, available at <http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/> (last visited May 4, 2008).

<sup>2</sup>Johnette Hassell & Susan Steen, *Demystifying Computer Forensics*, L.A. B. ASS’N J. (Dec. 2002), available at [http://electronicevidenceretrieval.com/demystifying\\_forensics.htm](http://electronicevidenceretrieval.com/demystifying_forensics.htm) (last visited May 4, 2008).

<sup>3</sup>Dictionary.com, *Merriam-Webster’s Dictionary of Law*, available at <http://dictionary.reference.com/browse/forensic> (accessed Jan. 19, 2007).

<sup>4</sup>*Plasse v. Tyco Electronics Corp.*, 448 F. Supp. 2d 302 (D. Mass. 2006).

<sup>5</sup>*Communications Center, Inc. v. Matthew Hewitt*, 2005 WL 3277983 (E.D. Cal. Apr. 5, 2005).

<sup>6</sup>A commercially available secure deletion application.

<sup>7</sup>See also Johnette Hassell & Susan Steer, *Preserving and Protecting Computer Evidence*, 3 EVIDENCE TECH. MAG. 4, 16-18 (July/Aug. 2005).

<sup>8</sup>THE NEW E-DISCOVERY RULES: AMENDMENTS TO THE FEDERAL RULES OF CIVIL PROCEDURE SCHEDULED TO TAKE EFFECT DEC. 1, 2006, at 30-31 (Dahlstrom Legal Publ’g Inc. Harv., MA 2006).

<sup>9</sup>FED. R. CIV. P. 26(f) (emphasis added).

<sup>10</sup>Ameriwood Ind., Inc. v. Liberman, 2006 WL 3825291 (E.D. Mo. Dec. 27, 2006).

<sup>11</sup>In re Old Banc One Shareholders Sec. Litig., 2005 WL 3372783 (N.D. Ill. Dec. 8, 2005).

<sup>12</sup>Jonathan W. Hughes & Simon J. Frankel, *E-Discovery: Pre-Litigation Considerations for In-House Counsel* (Nov. 22, 2005) (citing *Coleman (Parent) Holdings, Inc., v. Morgan Stanley & Co., Inc.*, 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005), 2005 WL 67885 (Mar. 23, 2005)). *See also* *DaimlerChrysler Motors v. Bill Davis Racing, Inc.*, 2005 WL 3502172 (E.D. Mich. Dec. 22, 2005).

<sup>13</sup>*Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 432-34 (S.D.N.Y. 2004) (hereinafter *Zubulake V*), (emphasis added).

<sup>14</sup>*Id.* at 431-32.

<sup>15</sup>*See* [www.equivio.com](http://www.equivio.com) (last visited Mar. 3, 2008).