



# **E-DISCOVERY HURRICANES:**

*How to Weather The Storms,  
Harness Their Power, and  
Stay on Course During Litigation*

by

**Brooks A. Richardson  
Fellers, Snider, Blankenship,  
Bailey & Tippens, P.C.**

**OBA Solo and Small Firm Conference  
Tanglewood Resort  
June 22, 2006**

## **E-DISCOVERY HURRICANES:**

### ***Basic Steps For Weathering The Storms, Harnessing Their Power, And Staying On Course During Litigation***

The digital information age is well upon us. In 1996 -- more than a decade ago -- technology industry experts estimated that 35 percent of corporate communications took place electronically.<sup>1</sup> In 2000, it was estimated that U.S. workers were sending more than 25 billion e-mail messages each day.<sup>2</sup> In 2003, industry experts reported that at least 30 percent of all corporate records were kept only in electronic form.<sup>3</sup> Today, the industry reports that North American businesses create an excess of 3.25 trillion e-mails per year and generate more than 90 percent of their information in digital form.<sup>4</sup> Most small businesses with more than fifteen employees have electronic storage capacity equivalent to 2,000 four-drawer file cabinets.<sup>5</sup>

The collision of the digital information age with the world of litigation has spawned a potential for litigation “storms” akin to the hurricane seasons that brought us Andrew, Ivan, Katrina and Rita. E-discovery in litigation is certainly akin to a hurricane – a mass of swirling issues and disputes that have the potential to destroy cases, send lawyers and litigants wildly off course, and cost incredible amounts of money. But there is good news. Hurricanes, unlike tornadoes, are fairly predictable. The e-discovery hurricane can be predicted, prepared for, and, potentially, even controlled and harnessed.

Like the lessons from Rita and Katrina, case law from litigation such as *Zubulake v. UBS Warburg* and *Williams v. Sprint/United Mgmt. Co.*, and recent amendments to the Federal Rules of Civil Procedure have provided us with basic steps for weathering the storms of e-discovery, harnessing their power, and staying on course during litigation. This article attempts to summarize those basic steps.

#### **I. STEP ONE: *Do not ignore the potential that an e-discovery hurricane will arise.***

##### **A. The Use Of ESI Is Pervasive.**

Electronically stored information (“ESI”) is now everywhere. Business deals are now commonly negotiated and documented by e-mail; workers attend meetings by video conference, employees keep calendars on desktop computers and PDAs; electronic task lists dictate workdays; phone handsets reveal the identities of past and present callers; security systems generate records of access to buildings.

ESI is not simply an “image” of a document, like a “PDF” or “TIFF” image, nor is it only the electronic bytes of data that reside in conventional computers and servers. ESI is

“any type of information that can be stored electronically.” Fed. R. Civ. P. 34. Consider the numerous sources of ESI now commonly found in our world:

| <b>COMMON SOURCES OF ESI</b>                  |  |
|---|--|
| Desktop computers                             | Event Data Recorders<br>(Black Boxes)              |
| Laptop computers                              | Internet Service Providers                         |
| Computer servers                              | Emergency Communications<br>Systems (i.e., Onstar) |
| Handheld computers                            | Mobile phones                                      |
| Medical devices                               | Digital voicemail                                  |
| GPS units                                     | Instant messaging databases                        |
| Memory sticks                                 | Flash Drives                                       |
| CD-ROMs                                       | DVDs   |
| Surveillance cameras/devices                  | Digital recorders and cameras                      |
| DVRs, Satellite TV Receivers, and<br>“TIVO’s” | IPODs and MP3 players                              |

See ABA, *Amendments to Civil Discovery Standards*, Section 8(29) at <http://www.abanet.org/litigation/taskforces/electronic/home.html>.

**B. The Existence Of ESI Affects The Outcome Of Litigation.**

Not only is the use of ESI pervasive, but the existence of ESI has a much greater likelihood of producing the “smoking gun” that affects the substantive outcome of litigation. This is true for a number of reasons. First, electronic data is created each time a computer or other electronic storage device is used. Computers generate automatic logs when they are used. Event data recorders, which are now in most new vehicles, and GPS units, keep automatic records of where the units have been and the routes of travel over which the units have moved. These vast amounts of data are potentially smoking guns that previously did not exist. Second, many forms of electronic data are unseen and unknown by users, making it less easy to “cover your tracks.” Third electronic data is difficult to destroy. A computer user who “deletes” files and e-mail messages is not actually erasing the data from the computer system, but simply marking the file as space that can be overwritten as needed. The space may never be overwritten. Fourth, manually-created ESI, such as e-mails, electronic calendar entries, digital pictures and recordings, has an “informal” quality that tends to cause users to exercise less discretion in their language and behavior. Many people now take pictures with their “easily deletable” digital cameras that they would not have taken with 35mm film that had to be developed by a third-party. Individuals say things in informal e-mails they might never say in formal letters or memoranda.

Many recent cases illustrate the importance of electronic evidence. The United States Justice Department found Bill Gates' e-mails in which he discussed his plans to undercut competition. In 2000, plaintiffs attorneys in a securities fraud case discovered an e-mail written by Henry Blodget, a Merrill Lynch stock analyst, in which Blodget made derogatory references to the tech stocks he had touted to investors. The case settled for over \$100 million. In May 2004, an age discrimination case against Gulfstream Aerospace Corporation settled for \$10 million after an electronic version of a paper was found on the computer of the company's plant manager (the decision-maker who began firing the company's older workers) discussing the "problems" of the company's aging workforce. The same month, a federal jury convicted former investment banker Frank Quattrone of obstructing justice and witness tampering after a trial that hinged on Quattrone's e-mail encouraging his colleagues to destroy files.

**C. The Risks and Consequences Of Spoliation Of ESI Are Significant.**

While the potential benefits of discovering the electronic smoking gun are obvious, the risks and consequences of ignorance about ESI are far worse than missing a potentially helpful or harmful document.

Courts have sanctioned parties and their attorneys for intentionally or negligently destroying or altering ESI, or failing to prevent its destruction or alteration. *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 (10<sup>th</sup> Cir. 2000) (imposing \$10,000 sanction for failing to search or preserve the e-mail of five key employees); *Prudential Ins. Co. of America Sales Practices Litigation*, 169 F.R.D. 598 (D. N.J. 1997) (imposing \$1 million sanction for failure to initiate comprehensive document management plan in response to court order to preserve all potentially relevant information); *RKI, Inc. v. Grimes*, 2001 WL 1654536 (N.D. Ill. Dec. 21, 2001) (ordering defendant to pay \$100,000 in compensatory damages and \$150,000 in punitive damages on default judgment after finding that defendant intentionally defragmented home computer to prevent plaintiff from learning he had deleted confidential information). A party's failure to honestly apprise the court of its computer capacity and ability to retrieve electronic data also can have serious consequences. *GTFM, Inc. v. Wal-Mart Stores, Inc.*, 2000 WL 335558 (S.D.N.Y. Mar. 30, 2000) (imposing \$109,753 sanction and ordering on-site inspection after discovering defendant's misrepresentation about its computer capacity); *Coleman Holdings v. Morgan Stanley & Co.*, No. CA-0305045 AI (March 23, 2005) (imposing a \$1.5 billion judgment against investment firm Morgan Stanley because it failed to produce thousands of potentially relevant backup tapes after telling the court no such tapes existed). Further, ignorance about ESI can lead to production of "hidden" privileged data that might lead to a blanket waiver of the attorney-client privilege, attorney work product doctrine, or other evidentiary privileges.

Given the pervasive use of ESI in our society, and its potential affect on the outcome of litigation, lawyers can no longer afford to ignore the potential for e-discovery storms in our cases, or be illiterate when it comes to ESI. Whether we are representing plaintiffs or defendants, the likelihood that we will need to obtain or review ESI is extremely high. We

all must know how to consider the existence of ESI, formulate and respond to discovery requests for ESI, gather, examine and produce ESI, and turn ESI into useable evidence in motions and at trial.

**II. STEP TWO: *Prepare For The Potential Storms By Learning Basic Survival Strategies.***

Appreciating the risk of potential storms is only part of the battle. To prepare for the e-discovery hurricane before it strikes, lawyers must learn and understand the basics of at least three things: (i) the basic types of ESI; (ii) the basic legal framework for identification, preservation and discovery of ESI; and (iii) the basic methods for obtaining, receiving and reviewing ESI.

**A. The Basic Types Of ESI**

Beyond simple definitions, perhaps the best way to learn and understand the basic types of ESI is to categorize them according to their various stages of accessibility, and to think of them in the same way we traditionally think of paper storage:

***STAGES OF ACCESSIBILITY***

|                         | <b>Paper</b>                | <b>User-created<br/>E-mail and Data</b>         | <b>Background /<br/>Replicant Data</b><br><i>(These exist at<br/>every stage)</i> |
|-------------------------|-----------------------------|---|---|
| <b>Most Accessible</b>  | Desks                       | “Active” e-mail / data                          | Metadata<br>Automatic copies<br>Cookies / cache files                             |
|                         | In-office file cabinets     | “Near-line” data                                |   |
| <b>Accessible</b>       | Off-site storage facilities | Backup / Offline / Archived data<br>Legacy data |   |
| <b>Least Accessible</b> | Trash /recycle bins         | Residual data                                   |   |
|                         | City dumps<br>Shredders     | Fragmented / damaged /<br>erased data           |   |
| <b>Inaccessible</b>     | Incinerated                 | Reimaged / wiped / scrubbed data                |   |

### ***ESI DEFINITIONS***

- Active data:*** Active data is information residing on the direct access storage media of computer systems, which is readily visible to the operating system and/or application software with which it was created and immediately accessible to users without restoration or reconstruction.
- Near-line data:*** Near-line data is information stored on removable media that can be accessed for active use. Typical examples would be CD-ROMs, DVDs, Zip Drives, and Floppy Disks.
- Backup data:*** Backup or offline data is information typically stored on removable optical disks or magnetic tapes for disaster recovery or archival storage where the necessity of retrieval is minimal. The main difference between near-line data and backup data is that backup data is not stored in a manner that will allow easy retrieval of individual documents and files.
- Legacy data:*** Legacy data consists of information that has been created or stored by the use of software and/or hardware that has become obsolete or replaced, and which cannot be accessed with current software.
- Residual data:*** Residual data is information that appears to be gone, but is still recoverable from the computer. It consists of “deleted” files to which the reference has been removed from the computer’s directory listings and file allocation table, but which have not yet been overwritten or re-imaged.
- Fragmented data:*** Even files that are overwritten may not be completely destroyed. The information comprising a single file may be scattered over multiple sectors on a computer drive. It is possible that some fragments of residual data can be overwritten, while other fragments are not.
- Reimaging or Scrubbing:*** This is the only way to definitively ensure electronic data is uniformly overwritten and unrecoverable.
- Replicant data:*** Operating systems and applications regularly create copies of files in order (1) facilitate recovery, (2) improve performance; or (3) perform a routine operation. These files are sometimes described as “file clones,” or “temporary files.” Later, they are “deleted” by the application or operating system, but the data left over from this process may still reside on the hard drive.

- Background data:*** Background data is a “catch-all” term for data that a computer system can create about documents or the computer’s use. This includes “metadata,” “audit trails,” “access control lists,” and temporary “cache files” and “cookies” from internet use.
- Metadata:*** Metadata, or embedded data, is computer-generated information about a particular data set or document that describes how, when, and by whom it was collected, created, modified, printed, and how it is formatted.
- Audit trails:*** Audit trails contain information about who accessed a computer, when access occurred, and for how long, what information was accessed, and whether any modifications were made to the accessed information, including the downloading of accessed information.
- Access Control Lists:*** Access control lists are used to limit employee access to a company’s computer systems in such a way that the lists can describe who has access to particular information.
- Cache files:*** When a computer user visits an internet sit, images are downloaded onto the hard drive to optimize performance, in “cache files.” A history of internet sites is also maintained on the computer.
- Cookies:*** Cookies are information about a computer user placed into a file by a website operator when the user visits that site.

## **B. The Legal Framework For Discovering ESI**

### **1. Important And Developing Law On E-Discovery.**

#### **ESI is unquestionably discoverable in litigation**

- *Armstrong v. Executive Office of the President*, 1 F.3d 1274 (D.C. Cir. 1993) (holding that electronic records of messages contain more information than paper printouts)
- *Crown Life Insurance Co. v. Craig*, 995 F.2d 1376 (7th Cir. 1993) (upholding sanctions to a party for failing to produce electronic data because “documents” under Rule 34 includes computer data)

- *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp. 1050 (S.D. Cal. 1999) (“The Court finds that by requesting ‘documents’ under Fed.R.Civ.P. 34, plaintiff also effectively requested production of information stored in electronic form.”)
- *Santiago v. Miles*, 121 F.R.D. 636 (W.D.N.Y. 1988) (noting that “a request for raw information in computer banks is proper and the information is obtainable under the discovery rules).

Parties and their attorneys must preserve ESI and may be sanctioned for negligent or intentional spoliation

- *Section 802 of Sarbanes Oxley Act, 18 U.S.C. § 1519* (requiring retention of corporate audit records and imposing criminal penalties for knowing spoliation)
- *Equal Credit Opportunity Act Regulations, 12 C.F.R. § 202.12* (requiring retention of records if creditor is on notice that an action is being taken for violation)
- *Equal Employment Opportunity Act Regulations, 29 C.F.R. § 1602.14* (requiring retention of employment records until final disposition of discrimination claim)
- *ABA Model Rule of Professional Conduct 3.4* (stating that an attorney shall not “unlawfully obstruct another’s access to evidence or unlawfully alter, destroy, or conceal a document or other material having potential evidentiary value . . . [or] counsel or assist another person to do any such act.”).
- *Oklahoma Rule of Professional Conduct 3.4* (same)
- *Telecom Int’l Am. Ltd/ v. AT&T Corp.*, 189 F.R.D. 76, 81 (S.D.N.Y. 1999) (“Once on notice, the obligation to preserve evidence runs first to counsel, who then has a duty to advise and explain to the client its obligations to retain pertinent documents that may be relevant to the litigation.”).
- *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D. N.Y. 2003) (Zubulake IV) (“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.”).
- *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004) (Zubulake V) (granting adverse inference instruction and holding that once litigation is reasonably anticipated, “a party and her counsel must make certain that all sources of potentially relevant evidence are identified and ‘placed on hold’ to the extent required in *Zubulake IV*” and that counsel must not only make the client aware of the obligation, but must also monitor compliance and facilitate production).

- *E\*Trade Securities LLC v. Deutsche Bank AG*, 230 F.R.D. 582 (D. Minn. 2005) (holding that document retention policy cannot be created primarily to eliminate foreseeably discoverable litigation).
- *But see Arthur Andersen LLP v. United States*, 544 U.S. 696 (2005) (holding that document retention policies “are created in part to keep certain information from getting into the hands of others, and that this in and of itself is a normal and permissible business practice.”).
- *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 (10<sup>th</sup> Cir. 2000) (imposing \$10,000 sanction for failing to search or preserve the e-mail of five key employees).
- *Prudential Ins. Co. of America Sales Practices Litigation*, 169 F.R.D. 598 (D. N.J. 1997) (imposing \$1 million sanction for failure to initiate comprehensive document management plan in response to court order to preserve all potentially relevant information).
- *RKI, Inc. v. Grimes*, 2001 WL 1654536 (N.D. Ill. Dec. 21, 2001) (ordering defendant to pay \$100,000 in compensatory damages and \$150,000 in punitive damages on default judgment after finding that defendant intentionally defragmented home computer to prevent plaintiff from learning he had deleted confidential information).
- *Leon v. IDX Systems Corp.*, 464 F.3d 951 (9<sup>th</sup> Cir 2006) (entering dismissal of suit as sanction to Plaintiff for running hard drive “wiping” program on business laptop that erased 2,200 files)
- *3M Innovative Properties Co. v. Tomar Electronics*, 2006 WL 2670038 (D. Minn. 2006) (granting adverse inference instruction and deeming certain facts established as sanction for failure to establish litigation hold, resulting in loss of e-mails).
- *Consolidated Aluminum Corp. v. ALCOA, Inc.*, 2206 WL 2583308 (M.D. La. 2006) (denying adverse inference instruction for negligent failure to suspend automated e-mail deletion program for litigation hold).

Litigants may be entitled to production of ESI in its native electronic format and to inspection of electronic data storage devices

- *Zhou v. Pittsburgh State University*, 2003 WL 1905988 (D. Kan. Feb. 5, 2003) (requiring production in electronic form after data previously provided in hard copy)
- *Northern Crossarm Co. v. Chemical Specialties, Inc.*, 2004 WL 635606 (W.D. Wisc. March 3, 2004) (holding that a party must produce electronic data in the form requested, but not requiring electronic production after party had already produced

- documents in hard copy and the requesting party had not specified the form of production).
- *In re Payment Card Interchange Fee and Merch, Disc. Antitrust Lit.*, No. MD-05-1720, 2007 WL 121426 (E.D.N.Y. Jan. 12, 2007) (reasoning that a party may provide ESI as maintained in ordinary course or in a form that is “reasonably useable” but does not “significantly degrade” searchability, the court held that conversion of native files to .tiff or .pdf format would degrade searchability).
  - *Palgut v. City of Colo. Springs*, No. 06-CV-01142, 2006 WL 3483442 (D. Colo. Nov. 29, 2006) (issuing discovery order providing that native format is the default form of production, though producing party has right to object).
  - *In re NYSE Specialists Sec. Lit.*, No. 03-CV-8246, 2006 WL 1704447 (S.D. N.Y. June 14, 2006) (production order specifying that hard copy documents must be produced in .tiff format, and ESI must be produced in native format, with metadata intact).
  - *Hagenbuch v. 3B6 Sistemi Elettronici Industriali*, No. 04-C3109, 2006 WL 665005 (N.D. Ill. March 8, 2006) (holding that production of ESI and emails in .tiff format was not acceptable due to lack of metadata and impaired search capabilities, and anti-tampering and difficulty in applying Bates numbers to native files were insufficient to justify production in .tiff format).
  - *Nova Measuring Instructions, Ltd. v. Nanometrics, Inc.*, 417 F. Supp. 2d 1121 (N.D. Cal 2006) (holding that production must be in native format, with metadata intact).
  - *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp. 1050 (S.D. Cal. 1999) (ordering defendant to make her computer hard drive available for inspection).
  - *Gates Rubber Co. v. Bando Chemical Industry Ltd.*, 167 F.R.D. 90 (D. Colo. 1996) (allowing plaintiff to copy hard drive to try and retrieve information regarding files that employee of defendant admitted deleting).

#### Courts may or may not shift the cost of discovery of ESI to the requesting party

- *Haworth, Inc. v. Herman Miller, Inc.*, 1995 WL 465838 (W.D. Mich. April 20, 1995) (requiring producing party to create and pay for computer program necessary to access information contained on electronic filing system maintained by defendant)
- *Linnen v. A.H. Robins Co., Inc.*, 1999 WL 462015 (Mass. Super. June 16, 1999) (requiring defendant to shoulder cost of restoring and searching backup tapes that may contain responsive e-mail).

- *In re Brand Name Prescription Drugs Antitrust Litig.*, 1995 WL 360526 (N.D. Ill. June 15, 1995) (“[I]f a party chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk.”).
- *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D. N.Y. 2002) (enumerating eight-factor test to decide whether the cost of expensive data recovery should be split between parties in discovery: (1) specificity of requests; (2) likelihood of discovering information; (3) availability of information from other sources; (4) purposes for which responding party maintains the requested data; (5) relative benefits to the parties of obtaining the information; (6) total cost of production; (7) relative ability of each party to control costs and its incentive to do so; (8) the resources available to each party).
- *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D. N.Y. 2003) (Zubulake I) and *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D. N.Y. 2003) (Zubulake III) (applying a seven-factor test in determining to shift some costs of discovery to the requesting plaintiff: (1) extent to which requests were tailored to discovery relevant information; (2) availability of the information from other sources; (3) total cost of the production compared to the amount in controversy; (4) total cost of production compared to the resources available to each party; (5) relative ability and incentive of each party to control costs; (6) importance of the issues at stake; (7) relative benefits to the parties of obtaining the information).

## 2. *The New ESI Amendments To The Federal Rules.*

The electronic discovery amendments to the Federal Rules of Civil Procedure became effective on December 1, 2006. There were amendments to Rules 16, 26, 33, 34, 37, and 45 and revisions to Form 35. The amendments provide litigants and courts, even in state court litigation, with a standard set of rules/guidelines for handling e-discovery issues.

*Rules 16(b) and 26(f) – Upfront Discussions About ESI Are Required:* These amendments require the parties to talk about electronic discovery at their initial Rule 16 conference and discovery conference under Rule 26(f), and adds three topics that should be addressed: (1) disclosure, discovery and format of production of ESI; (2) preservation of potentially relevant ESI; and (3) whether the court should enter any orders encompassing agreements the parties may reach for asserting claims of privilege or protection as trial-preparation material after production (i.e., clawback agreements).

*Rule 26(a)(1)(B) – Initial Disclosures of ESI Are Required:* The amendment requires each party to make voluntary disclosures of the categories and locations of all ESI that may be used to support its claims or defenses. Additionally, “data compilations” is deleted as unnecessary because it is a subset of both documents and ESI.

Rule 26(b)(2)(B) – Relevant ESI That Is Not Reasonable Accessible May Not Be Discoverable: The amended rule provides that “[a] party need not provide discovery of [ESI] from sources that the party identifies as not reasonably accessible because of undue burden or cost.” This amendment also requires that information identified as not “reasonably accessible” must be difficult to access by the providing party for all purposes and not just litigation. Courts will likely expect litigants to tell them precisely why ESI is difficult to access or unduly expensive. Courts retain discretion to require discovery of ESI that is not reasonably accessible upon a determination that “good cause” outweighs the burden, considering the limitations of Rule 26(b)(2)(C). Thus, even if ESI is not ordinarily discoverable because it is not “reasonably accessible,” a party may still have a duty to preserve such information.

Rule 26(b)(5)(B) – Clawback of privileged material is permitted: The amendment allows a party, under certain circumstances, the right to demand return of privileged information that was produced without having asserted privilege or trial preparation protection. If a party has provided privileged or work product information in discovery, it may notify the receiving party and state the basis of the privilege claim. The receiving party must then (1) return, sequester, or destroy the information and (2) may not disclose to third parties until the claim is resolved. Either the producing party or the receiving party can present materials to the court under seal for determination regarding the privilege claim.

Rule 33 – Parties may answer interrogatories by referring to specific ESI: Rule 33(d) now allows for the option to produce ESI as well as paper documents in lieu of answering interrogatories. The information must be as readily accessible to the interrogating party as it is to the responding party. To satisfy these provisions with respect to ESI may require the responding party to provide some combination of technical support, information on software application, or other assistance.

Rule 34(b) – Parties may specify and object to the form of production: The amended rule permits a requesting party to specify the form in which ESI is to be produced and permits the responding party to object to that form and produce in the form in which ESI is ordinarily maintained or in “electronic forms that are reasonably useable.” Rule 34(b)(iii) also provides that absent agreement or court order, a “party need not produce the same electronically stored information in more than one form.”

Rule 37(f) – Sanctions and Safe Harbors for dealing with ESI: Under the amendment, absent “exceptional circumstances,” courts may not impose sanctions for failing to provide ESI lost as a result of routine, good-faith operation of an electronic information system. This attempts to address a necessary feature of computer systems, i.e. the recycling, overwriting, and alteration of ESI from normal use. Even when litigation is anticipated it can be hard to interrupt or suspend routine computer operations to preserve or isolate data without creating problems. The amendment provides limited protection against sanctions if ESI has been lost or destroyed due to routine operation if operation is in good faith. However, a litigant cannot destroy specific information or exploit routine operations to

preclude discovery. In some circumstances, good faith may require a party to suspend or modify routine operations if it is subject to a preservation obligation.

### **C. Methods For Obtaining, Producing And Reviewing ESI**

Lawyers should have a basic understanding of the various production formats available for ESI, as well as options for management and review of those productions.

*Paper.* Paper production is familiar, easy to use, and simple to secure with bates stamps and watermarks. Boxes of paper may appear bulky and daunting, but flipping through large stacks of paper during a document review is often much faster than on-line review of images or documents in native format. But paper has its disadvantages. Paper takes up physical space. Paper is not searchable. Although paper can be scanned using optical character recognition (OCR) technology, that software requires additional time and money, and is generally only 80-90% reliable. (In other words, searches of documents that have been scanned using OCR technology will only find 80-90% of the documents that actually contain the search terms, because the characters were not properly recognized during scanning.) Further, paper is not well suited to display in an organized format the multitude of electronic information available.

*Electronic Images.* TIFF and PDF images are computer file formats for storing images. The primary advantages of these image formats is a blend of the advantages of paper with manageability and searchability. Although TIFF images are not searchable as produced, they are often produced with an associated text file that is searchable. PDFs can be made searchable. The images can be Bates-stamped electronically. Commercially available document management systems such as Summation, Concordance, and IConect, to name only a few, currently make imaging the most economical way to conduct and manage large amounts of paper production. When requesting or producing images, it is common to obtain a “load file” that eases the management of images by associating them with basic information, such as natural document breaks to tell where one document ends and another begins, text files (for OCR’ed images), and production Bates numbers.

However, image files, even with associated text, may not be sufficient. Such images are not designed to reveal metadata, and do not often reflect well the attachments to a document. With data compilations, such as spreadsheets, neither paper nor images can provide the same information as a document in native electronic format.

*Native Electronic Format.* Native format means files in the electronic format in which they were created and stored. E-mails may be maintained in their native format in collections (e.g., “.pst” files for Microsoft Outlook/Exchange) or as individual “.msg” files. A native format production can provide a reviewing party with the most information about relevant ESI, including its metadata, potential methods of data and format manipulation, and hidden macros that allow different electronic documents or components to work together. None of this information can easily be found in paper or image format.

However, producing and reviewing files in native electronic format is also a more expensive, time-consuming, and burdensome method of production. Native files cannot be managed easily in litigation, for multiple reasons. First, simply opening a native file to determine relevance can alter the metadata of that file and subject a party to sanctions. Thus, there is more expense in reviewing and copying native files for production. Second, native files cannot be Bates-stamped or watermarked for ease of tracking and securing. Producing parties often go to the expense of placing native files in an electronic folder marked as “Confidential” and with a Bates number, although this is hardly considered fool-proof security. Third, native files are susceptible to manipulation and tampering. While producing parties cannot “lock” their native files from being manipulated without risking spoliation, they can assure a means of determining if a native file has been altered by assigning an MD5 “hash mark” that is an algorithm consisting of the unique digital signature of the native file. With a “hash mark” it is possible to tell if a native file has been altered in any way. Fourth, to view files in native format, a litigant must have the software in which such files were created and stored. Fifth, the commercial technology for litigation management of native files is still developing, and is more costly than management of images.

In light of the costs of discovering documents in their native electronic format, litigants would be well-served to narrowly identify the types of documents they are willing to accept or produce in native electronic format, and ask for the rest in paper or image format. Such is likely to help keep costs down and judges satisfied.

*Computer Hard Drive Inspection:* Occasionally, and often in cases where witnesses acknowledge deletion of ESI, litigants will want or need to obtain the right to obtain residual data and metadata on a computer’s hard drive. To do this, a computer forensics expert must take a mirror image of the drive with an exact match of the computer’s MD5 hash. Such a process for a typical desktop computer could easily cost \$20,000, depending on the size of the computer’s hard drive, *before* any review has occurred for relevant information. Typically, review of a mirror image occurs through the use of negotiated word searches, with the potentially relevant data turned over to the producing party to review for actual relevance and privilege.

**III. STEP THREE: *Prepare your clients for the storms as soon as you know they are coming (and preferably even before).***

Most of us will not have clients who want to pay us to learn about and analyze their Information Technology infrastructure to advise them about how to survive e-discovery storms they cannot yet see. Unfortunately, for many business clients, that might be the best thing for them. The duty to preserve relevant evidence arises immediately when a party reasonably anticipates litigation, not after it is sued, finds counsel, educates counsel about the issues in dispute, and allows counsel to assess the potential universe of relevant data and advise it on what to preserve for litigation. The time between “Point A” (reasonably anticipating litigation), and “Point B” (after the lawyer has been able to assess the potential universe of relevant data and advise on preservation) can result in document destruction or

alteration that could potentially be very costly for the client. If a business client will permit (and pay for) e-discovery legal advice before an e-discovery hurricane is formed, it may ultimately save money if and when such a storm does arise.

In the typical circumstance though, we must move quickly after being hired for litigation to assess our clients' information technology infrastructure and counsel them on their duties to preserve relevant information. Regardless, the general steps are the same, to be used as applicable for businesses or individuals.

First, sit down with your client's key witnesses (or the individual clients themselves) to discuss how they use computers and technology, where they create and store data, and how they destroy or delete data. Obtain their e-mail addresses, cell phone information (providers and numbers), and home or personal computing information and habits. Ask about their internet service providers. Determine how they keep calendars, contact information, and other files. Find out if the individuals visit or participate in any networking websites, such as MySpace, FaceBook, or LinkedIn.

Second, get a copy of the business client's document retention policy, if they have one. In 2005, it was estimated that only 59% of companies had e-mail retention policies.<sup>6</sup> Pay close attention to how the policy handles electronic data. Most corporate retention policies do not adequately address electronic data. Find out if the client has instituted a litigation hold since the policy was written and, if so, what successes and problems occurred.

Third, sit down with the business clients' information technology employees or consultants and ask them to explain, as if you were a sixth grader, how electronic information is processed through the clients' information technology infrastructure. What backup devices are used? What storage capacity? If applicable, discuss their knowledge of the document retention policy and how they operate their systems within the policy. Ask for or create a flow chart of the storage points for ESI during your discussions. Once you know the storage points for ESI, ask how long information is stored at that particular point in the process. Pay close attention to the IT budget and ask questions about the potential impact of a litigation hold on that budget.

Fourth, issue and reissue a preservation letter to the client in the event you are on notice of the client's potential litigation. The litigation hold letter should be specifically tailored to the facts and circumstances of the case, and should be issued to all employees who may have relevant information, not simply to the key contact persons. The letter should discuss the types of data that should be kept, how it should be kept, and the potential consequences for failure to preserve. The letter needs to provide contact information for employees or data custodians if they have any questions. The contact may need to be an attorney contact as well as a technical contact for assistance with hardware or software issues. The letter should ask recipients to help identify any relevant information or persons who might have relevant information. The letter should be marked "Attorney-client privilege" and "Confidential."

Fifth, continue to monitor the clients' compliance with the litigation hold. Send follow-up reminders of the hold. Contact the everyday data custodians who are creating and storing data to ensure they understand how to comply with the litigation hold. Document your conversations and efforts. Determine if employees are leaving the client to be sure no information is lost when the employee leaves. Consider asking employees to sign a form stating that they have read, understand, and will comply with the litigation hold to the best of their ability. This can cause employees to take their role in data preservation a little more seriously, and serve as back-up documentation of your good faith efforts to enforce the litigation hold.

#### **IV. STEP FOUR: Meet The Storm Head-On.**

##### **A. Engage In Early Dialogue.**

The new amendments to the Federal Rules require parties to discuss ESI at the outset of litigation (Rules 16(b) and 26(f)). Even if this were not required, it is the best way to survive a potential e-discovery hurricane. Actively engaging in an early dialogue about the discovery of ESI can avert costly disputes over broad discovery requests, the format of production, and the need for duplicative production (i.e., paper and native format).

When discussing the need for searching, preserving, disclosing and producing ESI, parties should discuss, at a minimum the: (a) time periods that data remains accessible or potentially retrievable in a client's electronic infrastructure; (b) the ESI and computer usage and storage habits of the likely witnesses and persons with knowledge; (c) the ESI most likely to be found and/or requested relevant to the claims or defenses asserted and the location and format of such data; and (d) the key search terms that should be used to find relevant ESI.

##### **B. Follow The General Steps Of All Discovery.**

Whether we are requesting or responding to discovery, and whether the information at issue is electronic or traditional, the basic discovery steps remain the same:

| <b>Requesting</b>           | <b>Responding</b>            |
|-----------------------------|------------------------------|
| Analyze and plan            | Analyze and plan             |
| Warn                        | Preserve                     |
| Formulate Requests          | Formulate Responses          |
| Obtain and Review           | Review and Produce           |
| Cooperate or seek to compel | Cooperate or seek to protect |

The most important of all these steps in the world of electronic discovery is analyzing and planning, because all other steps flow from this one. What electronic information is likely to be needed? What are the likely sources of electronic information? In what formats are the electronic information kept? What requests will be most likely to target relevant ESI?

How can the ESI be managed? How will privilege determinations be made? What are the likely disputes and costs? What compromises are possible?

All of these questions should be asked carefully, and early, to create the best possible chance of weathering an e-discovery hurricane.

**V. STEP FIVE: *Harness The Storm's Power By Engaging In Fair E-Discovery.***

**A. Formulate Targeted Requests To Discover Information About The Opposing Party's Potential Sources of Relevant ESI.**

1. Ask for a network map, which will show all available resources.
2. Ask what operating systems are being used. This will tell you what logs are available.
3. Ask for a list of all software applications used.
4. Ask for the policies and procedures for backing up files and data.
5. Ask for the retention policy for electronic data.
6. Ask for any litigation hold notices.
7. Request an inventory of all computer devices.
8. Determine what type of monitoring software may have been installed on computers.
9. Request e-mails in electronic format (bit stream image), not hard copy, so that you can see headers, bcc info, etc.
10. Request a list of e-mail mailboxes and the sizes of the e-mails contained in those boxes.
11. For Microsoft Exchange servers, request the log file, which usually contains text for all e-mails for approximately one year. (While it may not hold the actual attachments, information regarding the attachments will be included).
12. Find out if a third-party e-mail service is used from which you may be able to recover e-mail.

13. If you are told that a hard drive has been “wiped,” find out which software program was used, and how. Not all programs wipe the entire drive, and information can still be retrieved.
14. If requesting a “ghost” or “mirror” image of a computer’s hard drive, be sure that it is set to grab the data byte for byte. Request a bit-stream image, which copies from the beginning to the end of a drive.

**B. Ask Routine Questions About ESI in Depositions**

1. Do you use e-mail at work? At home?
2. What e-mail accounts do you have?
3. Do you use your personal e-mail accounts for work?
4. Do you work at home on a computer?
5. Do you use a laptop . . . PDA . . . Blackberry . . . pager?
6. Do you still have your old computer? Who did you give it to?
7. Have you ever deleted an e-mail or other document concerning . . .?
8. Why did you delete it?
9. Have you ever asked your IT folks to retrieve a deleted document? Were they successful?
10. Have you ever made hard copy printouts of your e-mail?
11. Have you ever exported e-mail to a database in locations other than the e-mail program?

**C. Consider Asking For a 30(b)(6) Deposition Concerning ESI.**

Often, a deposition of the party’s most knowledgeable person concerning the party’s information technology infrastructure, data storage, and retention will be the most valuable method for determining the potential existence of relevant but unproduced ESI.

An MIS or IT manager will likely know what types of computers and software are being used; the type of network and its configuration, what password and encryption technology is employed; how the voice mail system is configured; how the computer system attaches to the Internet, backup procedures for software and data, and any data retention policies. Deposition of IT administrators may uncover “forgotten evidence,” such as backups

retained in contravention of retention policies, old computers, and copies of hard drives made when drives are upgraded.

Consider including the following topics in a corporate deposition notice concerning the opposing parties ESI:

**TOPICS ON WHICH DEPOSITION EXAMINATION IS REQUESTED**

1. a. The efforts made by XYZ Co. to supply its Designated Representative(s) with all information requested in its notice which is known or reasonably available by XYZ Co.
- b. Identification of the sources of all such information including the names and titles of all persons supplying any such information and a description of all records used to ascertain or verify such information.
2. The organization and staffing of XYZ Co.'s management information services department.
3. XYZ Co.'s document and data retention and preservation policies and procedures, document storage systems, data storage systems, document and data retrieval systems, and the methods of storage (including but not limited to e-mail, computer data bases, microfiche and micro film) for documents and categories of documents relating to \_\_\_\_\_.
4. The existence and nature of XYZ Co.'s systems and procedures for backing up electronically stored information.
5. The nature and architecture of XYZ Co.'s internal computer networks, local area networks and wide area networks.
6. The existence, nature and location of data storage devices upon which electronic data generated by XYZ Co. may be stored.
7. The identities and locations of all sites remote from XYZ Co.'s premises which store electronic data for XYZ Co.
8. The nature of the operating systems and other software used by XYZ Co. for the operation, control and maintenance of internal computer networks, intranets, local area networks, wide area networks, personal information managers, e mail systems and data storage and retrieval systems.

9. The nature of the applications software used by XYZ Co. for word processing, e-mail, data base creation and management, \_\_\_\_\_ [name other specific applications].
10. The nature of the server log systems used by XYZ Co.
11. The nature of XYZ Co.'s systems for file protection and encryption.
12. The identities of the individuals who could provide access code, if required to do so.
13. XYZ Co.'s procedures for purging storage devices or directories and revocation of access codes and passwords upon the termination of the employment of an employee.
14. XYZ Co.'s procedures for treatment of computers and storage devices prior to sale, disposal or other disposition.
15. The identities of outside contractors, consultants or vendors used by XYZ Co. to upgrade hardware or software.
16. The identities of outside contractors, consultants or vendors used by XYZ Co. to develop or write custom or semi-custom software.
17. The identities of outside contractors, consultants or vendors used by XYZ Co. to assist with respect to any aspect of the management of XYZ Co.'s management information or data processing systems.
18. The existence, nature and location of hard copy or electronic logs of changes or modifications to applications software used by XYZ Co.
19. The steps taken by XYZ Co. since [the filing of this action] [the date of XYZ Co.'s acquisition of information indicating the possibility of assertion of the claims asserted in this action] [the date of the letter to XYZ Co. from counsel for \_\_\_\_\_, admonishing XYZ Co. to take steps necessary to safeguard and preserve XYZ Co.'s electronically stored documents and other data] to protect XYZ Co.'s electronically stored documents and other data from alteration or destruction.

**D. Consider Asking For A Computer Inspection Under Rule 34.**

If ESI is not being produced, or witness testimony suggests that ESI may have been deleted or destroyed, consider asking for a computer inspection under Rule 34. Such a request should be narrowly tailored to increase the likelihood of being granted and lower the costs of forensic discovery. Consider the following example for an inspection request:

Plaintiff requests that Defendant permit Plaintiff or her representatives to enter Defendant's premises at \_\_\_\_\_ and to inspect, test, sample, and copy data, records and files (including e-mail sent or received by Defendant and files located remote computer systems that may be accessed by Defendant's computer system(s)), on the hard drive(s), other storage devices, backup tapes, and in memory of the following computer systems and any other computer systems located on said premises: [list specific computer systems requested].

Remember that if such an inspection request is granted, a proper forensic examination requires "mirror" or "bit-stream" imaging to avoid destruction of metadata and allow for authentication at trial of any evidence obtained. You will need to hire an expert.

**CONCLUSION**

While the potential power of e-discovery is exciting, the swirling mass of e-discovery issues will continue threatening to overwhelm litigation for many years to come. Costs of discovery and recovery of electronically stored information, relevance and burden disputes, lack of technical knowledge by parties and lawyers, the potential for spoliation, and the overwhelming amount of electronic data available are all critical issues litigators will have to address in the world of electronic discovery. These e-discovery issues, like the warm waters and high winds that convert mere storms to tropical depressions to hurricanes, become more difficult and dangerous as the stakes and "heat" rise in particular cases. Regardless of our particular field or specialty in litigation, it is important that we obtain a base, core level of knowledge related to electronic discovery, and then use that knowledge to prepare for the potential storms.

---

**END NOTES**

<sup>1</sup> Peter Lacouture, *Discovery and the Use of Computer-Based Information in Litigation*, 95 Rhode Island B.J. 9, 9 (1996).

<sup>2</sup> Jeff Lendino, *Buried in the Bytes: The Coming Age of Electronic Discovery*, 17 Law PC 6 (July 15, 2000).

<sup>3</sup> International Data Group, Inc. as cited in [www.internetnews.com/IAR/article.php/1471801](http://www.internetnews.com/IAR/article.php/1471801); Barsocchini, *Electronic Data Discovery Primer*, Law Technology News at 21 (American Lawyer Media, Inc., August 2002).

<sup>4</sup> Bradford S. Babbitt and Kori E. Termine, *The New Reasonable Accessibility Standard: What's So Reasonable About It?*, e-Discovery at 42 (ABA 2007).

<sup>5</sup> Jason Krause, *e-Discovery Gets Real*, ABA Journal at 46 (Feb. 2007).

<sup>6</sup> Sue Reisinger, *Electronic Company*, Corp. Couns., October 2005, 100 at p. 104.