Finding the smoking gun: A hands-on guide to dealing with electronic discovery

With the advent of metadata, pushing the "delete" button does not erase damning e-mails or documents

Solange E. Ritchie

Let's face it, electronic gadgets are everywhere. As you read this article, your teenager is text-messaging a friend on her new "smart" phone. Even though you are on your way home, you just responded to office e-mails from your Blackberry or Treo. There is a "smart" card or "zip" drive in your briefcase with this evening's work or the day's e-mails to review. And of course, let's not forget your portable laptop which "syncs" up with both your home desktop computer, if you still have one of those dinosaurs, and your office's network computer.

These are just a few of the possible sources of electronic discovery or what the Federal Rules of Civil Procedure now call "electronically stored information"[1] or ESI. The paper trail, or should I say, the electronic data trail, is almost endless. The average business person gets and sends between 50-150 e-mails a day. Multiply that by 365 days a year and a company with 100 employees, and you get the picture.

A single CD-ROM, with 650 megabytes, can hold up to 325,000 typewritten pages. The smallest 20 gigabyte iPod can hold over three million pages of word documents. The volume of electronically-stored data is exploding and shows no signs of slowing. ESI data and related discovery can be a godsend in litigation, or it can be your worst nightmare, both for the sheer volume of it and the client cost.

ESI discovery can overwhelm opponents or be used to hide a needle in a haystack. As a practical example, remember the Bush administration's embarrassment over the Michael Brown e-mails, as the head of FEMA, during the Katrina disaster? That was just the plain e-mail itself! No metadata was exposed to the public through the media. Now imagine that single e-mail as part of an e-mail string, which when forwarded to all users, inadvertently discloses attorney-client communications.

Electronic discovery is a growing concern for businesses and corporations. As a lawyer, how do you control enormous costs and burden associated with e-mail? As businesses increase the use of electronic communication, so does the need for counsel to understand how to preserve, effectively obtain, and avoid sanctions related to inadvertent destruction of electronic or digital discovery.

This article will discuss two areas of concern in responding to these questions. One is forensic analysis and the other is electronic discovery, which has been around for quite some time in federal practice and has recently been codified to some extent in the recently amended Federal Rules of Civil Procedure (hereinafter FRCP), effective December 1, 2006. This article will concentrate on FRCP Rule 16 and 26 amendments and discuss the major case that led to these amendments: *Zubulake v. UBS Warburg LLC* (Zubulake I) and its progeny line of cases, including *Zubulake v. UBS Warburg LLC* (Zubulake V) (S.D.N.Y. 2004) 229 F.R.D. 422.

Forensic analysis: The beginning of your discovery plan

So, where do you start? First, hire a forensic computer specialist. While this can be an expensive proposition, it can be worth it when one considers that they can help you obtain that hidden "smoking gun" often found in metadata.[2] Metadata is electronic data contained in documents prepared with programs such as Microsoft Word or WordPerfect. The latest edition of Merriam-Webster's College Dictionary defines *metadata* as "data that provides information about other data." The advisory committee note to the Federal Rules of Civil Procedure Rule 26(f), 28 U.S.C. describes metadata as: "Information describing the history, tracking or management of an electronic document." With the right software program and the right forensic analysis, metadata can reveal such crucial information as when a document was created, who created it, the substance of the original document, all changes to a document, who made those changes, when

Copyright © 2007 by the author.
For reprint permission, contact the publisher: **www.plaintiffmagazine.com**

they were made and notes/comments to the document which do not appear in the final hard-copy version. Metadata can also reveal privileged and confidential information. Metadata should not be shared with opposing counsel or a competitor for these very reasons, yet companies who transmit Word and WordPerfect documents as e-mail attachments unwittingly share this harmful information each day.

How do you preserve confidentiality and deal with metadata in a non-litigation setting? How do you advise your corporate clients to deal with confidentiality headaches associated with metadata while preserving their ability to communicate with suppliers, manufacturers, clients and others? One solution is to use software programs, such as Metadata Assistant, commonly available on the Internet, to reveal and scrub metadata before a document is transmitted via e-mail attachment. The other solution is to convert documents to .tif or .pdf format and transmit, although this is not a solution if the recipient plans to do anything more than simply read the attached document.[3]

Copying and pasting a Word or WordPerfect document into an e-mail does not remove metadata. In litigation, once a preservation letter[4] is sent or an order to preserve discovery made by a judge, there is little that a company can do to obliterate metadata relevant to the litigation.

Another benefit to forensic analysis is the retrieval of data which the user may believe was deleted. Many people still believe that as you hit the delete button on an e-mail, that document can never be seen again. Not true. The same is true of documents that have been "saved over" or over-written. Simply put, without a concerted and very-knowledgeable effort to delete information on the part of the user, it is still there and can be retrieved. Deleted and over-written e-mails and documents remain easily accessible on a computer's hard drive. In the last two years, the level of affirmative steps necessary to successfully delete an item of ESI has increased dramatically. The number of over-writes to successfully obliterate electronic information continues to increase each year. A forensic expert can often obtain this "deleted" electronic information.

ESI hiding places: What every attorney should know

Not only is metadata a serious concern for employers and attorneys alike, counsel must expand their thinking regarding where ESI can be located. It is helpful to think of electronic discovery as more than your run-of-the-mill files on the computer work station or PC. Technology has expanded possible sources of electronic discovery. Often overlooked discovery sources of the "smoking gun" include: active data, thumb drives, outside recipients (hard drives, servers, backup), laptops and personal home computers, building access controls systems, workstation drives, server hard drives, e-mail servers, other drives (USB, external drives, MP3 players), dictation: audio tape, CD-ROMs, firewall and router logs, floppy disks, Internet postings, mainframe computer files, memory cards, minicomputer files, network server files, "recipient" e-mail messages, archived e-mails, undeleted and deleted files and messages, tape backup, voicemail messages, web-based e-mail (i.e. "hotmail," etc.), zip and jazz drives, palm pilots and similar devices, digital phone records, smart cards, etc. A forensic expert can help you determine which of these information sources is most beneficial and cost- effective to mine.

Where the storage media is easily locatable and small, such as a desktop computer, it is usually better to have the media delivered to the expert for mirroring. Computerized data includes not only conventional information, but also operating systems (programs that control the computer's basic functions), applications (programs used directly by an operator, such as word processing and spreadsheets), computer-generated models, and other instructions residing in a computer's memory.[5]

Before actually entering an opposing party's premises, a judicial preservation order should be obtained to make sure that all sources of information, including primary, secondary and off-site computer files be preserved pending discovery.[6] The order should be as specific as possible to include all versions of possible data including e-mails, diaries, organizers, spread sheets, financial and commercial data computations and similar sources of information.[7] The identity of the system's management personnel should also be obtained.

If the electronic data is located offsite or in a larger scale, it is often more feasible for the expert to travel to the network site and conduct the "mirroring" of the hard drives there. By creating an exact duplicate of the original electronic material, the expert can guarantee that the original data is not corrupted. The expert can manipulate the imaged material in any number of ways by creating a mirror of the hard drive.

If copying of the network drive or information is done offsite, it is extremely important that the expert take careful note of who has handled the computers or network or transferred the material, so that there is no chain of custody issue later. To the extent that confidential material is disclosed during any mirroring, the retained computer expert should sign a confidentiality agreement.

Depending on the costs, "mirroring" all of the storage media on an entire network drive may not be feasible. A forensic expert can advise of the most cost-effective manner to obtain the most beneficial information. Because of the casual nature of e-mails, they are often a good place to start on a limited budget.

Since relevant electronic data may not be stored in an appropriately named file, it is important that the forensic expert conduct as broad a search as a

Copyright © 2007 by the author.
For reprint permission, contact the publisher: **www.plaintiffmagazine.com**

budget allows. In order to avoid allegations of spoliation of or tampering with evidence, the retained forensic expert should never actually touch the opposing party's computer system. Rather, the expert should direct his own employees to search for data, restore and search older files, observe any results and protect and preserve the authenticated copies of computer format data files, and as appropriate print out results.[8]

It is imperative that a forensic expert be hired early on. An expert can assist in helping the attorney draft discovery requests to obtain electronic data, can work with the attorney to establish pre-defined search parameters, draft probative discovery requests, and help retrieve relevant information from a great quantity of electronic computer-generated information. The expert can also pinpoint the types of discovery that are most likely to lead to the data that you need and possibly, through metadata, uncover that hidden "smoking gun."

Amended Federal Rule of Civil Procedure Rule 16(b) and Rule 26(f): Scheduling and planning for ESI discovery or disclosure

Under amended FRCP Rule 16(b)(5) and (b)(6), the parties to federal litigation now have an affirmative duty to address ESI in their Scheduling Order for the initial pre-trial conference. According to amended FRCP Rule 16(b), the parties must include "provisions for the disclosure or discovery of electronically stored information" and "any agreements the parties reach for asserting claims of privilege or protection as trial-preparation material after production." So attorneys need to be fully familiar with their clients' ESI related storage operations, computer systems, IT staff involved in access and storage of ESI, possible forms of ESI production, backup operations and the company's destruction policies and procedures and cost estimates for identification, retrieval and production.

It is also critical at this early stage that counsel obtain the names of key IT people at the client company and understand their roles in the dissemination, storage, archiving and retrieval of ESI. Key players must understand that it is critical that they effectively communicate with counsel on litigation-related issues.

Amended FRCP Rule 26(f) adds ESI-related topics to the initial discovery conference. First, counsel must address "issues relating to preservation of discoverable information," issues related to the discovery and form of ESI, and whether the court should enter an order allowing the assertion of privilege after production. The focus of both of these amended sections is early planning, scheduling and client communications related to ESI to prevent the inadvertent destruction of relevant evidence.

Amended Federal Rule of Civil Procedure Rule 26(b)(2)(B): Limitations on scope of ESI production and accessibility

Mirroring *Zubulake v. UBS Warburg, LLC* (S.D.N.Y 2003) 217 F.R.D. 309, 311 (*Zubulake I*), FRCP Rule 26(b)(2)(B) provides that a party need not produce ESI that is not "reasonably accessible because of undue burden or cost," unless ordered following a motion to compel where the requesting party has shown good cause for the production.[10] So the producing party has the initial burden to show ESI is not reasonably accessible because of undue burden or cost. The amended rule does not state what is "inaccessible" evidence.[11] Presumably, the courts will consider the same factors indicated in *Zubulake I* at pages 318-319. Then the party seeking production must show good cause for production, using factors similar to those stated in *Zubulake I*, to wit:

- The specificity of the request;
- Whether the information is available from other sources (and the quantity of it);
- Failure to produce relevant information likely to have existed but no longer available through easily accessed sources;
- The likelihood of finding relevant information not obtained from other sources which can be easily accessed;
- The importance and use of the requested information;
- Its importance to the litigation; and
- The parties' resources.

Amended Federal Rule of Civil Procedure Rules 16 and 26(b)(2)(B): Privilege considerations and clawback agreements

The massive volume of ESI-related data and difficulties in reviewing information in electronic format has lead to the use of "clawback agreements." Amended FRCP Rule 16 allows that "any agreements the parties reach for asserting a claim of privilege or protection as trial-preparation material after production" can be included in the scheduling order. Amended FRCP Rule 26(b)(5)(B) states procedures for the inadvertent production of privileged information:

> If information is produced in discovery that is subject to a claim of privilege or protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specific information and any copies of it and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified of it, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved.

This mechanism places the issue in front of the court – which is what parties do anyway. Given the split among the

Copyright © 2007 by the author.
For reprint permission, contact the publisher: **www.plaintiffmagazine.com**

federal district courts in allowing clawback agreements, the amendment's effectiveness is questionable. These procedures also do not address the inadvertent disclosure to third parties who are not subject to the court's jurisdiction.

Problems with the amended federal rules dealing with ESI

These are just some of the changes to the Federal Rules of Civil Procedure for Rules 16, 26, 33, 34, 37 and 45. In addition to the problems identified above, Amended Rule 26 (b)(2)(B) shifts the costs of discovery as discussed above. Whether a source is "reasonably accessible" according to the amended rule, depends on whether obtaining the information involves "undue burden or costs." But how will the courts evaluate what they consider undue burden and costs? Of course, this wording presents at least four significant problems.

First, a party is charged with determining its own production responsibilities since they are based on the parameters that the party uses to determine whether information is "reasonably accessible." Conceivably, a party could avoid discovery by asserting that the storage media is not "reasonably accessible." Corporations may begin to re-characterize their electronic data by saving it in "inaccessible" forms to eliminate and/or avoid discovery of problematic material.[12] The amended rule offers no definition of what is deemed "reasonably accessible." Presumably, it is referring to the parameters in *Zubulake I* (S.D.N.Y. 2003). 217 F.R.D. 309, 318-320 Not all courts are following the *Zubulake* holding; some take a broader approach and others take a more narrow approach.[13] So this language is ambiguous and subject to manipulation.

Second, by allowing a party to make a good faith assertion that the data is "not reasonably accessible" and requiring the requesting party to file a motion stating that the data is "reasonably accessible," courts are placed in the position of refereeing a highly technical matter for which they are ill-equipped. Courts will be forced to rely on outside experts to opine as to whether the data is or is not "reasonably accessible." Such a battle obviously favors the party who is better funded and leaves the court at the mercy of that party's expert.

Third, the "good cause" burden on the requesting party is vague. It forces the requesting party to disclose in good faith, "a copy of, or a description by category and location of" potentially relevant data stored under Rule 26(a)(1)(B). What if a producing party fails to provide an accurate description, or worse, fails to disclose the existence of certain documents or data in the first place? This creates an imbalance because the requesting party will not know that the documents or data exist, thereby handicapping that party from showing good cause for the production of documents. The power is, once again, left in corporate hands to disclose the existence of the documents and/or data. It is entirely foreseeable that in a situation where a document is incriminating or damaging, a party, with the appropriate monetary resources to do so, may choose to *re*characterize, *mis*characterize, or fail to disclose the existence of the document or data, thereby making it difficult, if not impossible, for the parties and the court to ensure full and complete discovery.

This language may also lead companies to not upgrade outdated mainframe applications, which may be serviceable and usable internally, to prevent the production of problematic data based on a claim that it is "inaccessible" and too expensive to restore and produce. This places the power in the hands of the party litigant, instead of the courts. The new rules preclude sanctions for destruction of electronic discovery if a party can show that the destruction came about through "routine" use of their document retention systems. Similarly, amended Rule 37(f) creates problems:

> Absent 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 rule prohibits sanctions "absent exceptional circumstances." This safe harbor exception reflects a divergence from the common law spoliation doctrine and the prior federal rules which prohibit any destruction of documents, whether by intent or not. This standard encourages corporate defendants to recharacterize or mischaracterize data and create corporate policies to subvert data production. It does not reflect the holding of the *Zubulake I* and its progeny cases, discussed *supra*. It theoretically allows a corporate defendant to perform a "litigation hold" negligently, if the corporation can show the destruction was "a result of the routine, good-faith operation of an electronic information system." This rule also offers no guidance on what might be considered an "exceptional circumstance." Common law spoliation and the prior federal rules allow courts to punish the deliberate destruction of documents and data in an attempt to evade discovery, when they design bad storage systems or fail to effectively communicate the parameters of "litigation hold" order from the courts and then oversee that order's enforcement. The amended rule takes away this capability. Overall, the amended rules fail to adequately address spoliation issues.

In conclusion, the amended rules do not go far enough to quell possible ESI discovery abuse. But they are a start. It will be interesting to watch as the courts implement these new rules to see if they continue to rely on the *Zubulake* as a benchmark on ESI-related discovery. One thing is for sure, ESI related discovery is here to stay. It is up to counsel if it will be friend or foe in litigation.

Copyright © 2007 by the author.
For reprint permission, contact the publisher: **www.plaintiffmagazine.com**

Solange Ritchie works with the Law Offices of Steven R. Young, in Irvine. She received her B.A. from the University of Florida, Gainesville, 1986; J.D. Western State University College of Law, Fullerton, 1994. Ritchie has been involved in complex cases involving digital or electronic discovery in patent, trademark and copyright cases, as well as complex business disputes. She has represented entrepreneurs, start-up companies and major corporations and entities such as Carl Karcher Enterprises, Parkview Community Hospital, Crystal Cathedral Ministries and Farallon Gateway. Anthony v. Mazon, OCSC Case No. 03CC09517 was recognized as one of the Top Verdicts of 2005 in the Los Angeles Daily Journal. She can be reached at solange-ritchie@hotmail.com.


Ritchie

Endnotes:

[1] See Amended Federal Rule of Civil Procedure Rule 34 adding these words.

[2] This expert can also assist you to communicate the need for a litigation hold on ESI destruction, either purposeful or inadvertent, by your client.

[3] Courts are split on whether this type of production is sufficient. In *Hagenbuch v. SB6 Systemi Elettronici Industriali SRI*, 2006 WL 665005 (N.D. Ill. Mar 8, 2006) (court ordered production of documents in native format, because TIFF files did not include metadata or attachments and were not in the format maintained in the usual course of business); but see *Zakre v. Norddeutsche Landesbank Girozentrale,* 2004 WL 764895 (S.D.N.Y. Apr. 9, 2004) (the court held text searchable format of 200,000 e-mails sufficient if they were kept in the ordinary course of business).

[4] See Solange E. Ritchie, *Digital and Electronic Discovery: How to Preserve It, Obtain It and Avoid Sanctions Along the Way*, Forum, Published by the Consumer Attorneys of California, Volume 36, (Spring 2006).

[5] See generally Comment, *The Discovery of Electronic Data in Litigation: What Practitioners and Their Clients Need to Know*, 17 Wm. Mitchell Law Review 1825 (2001) and Meyer & Wraspir, *"E-Discovery" Preparing Client for (and Protecting Them Against) Discovery in the Electronic Information Age*, 26 Wm. Mitchell Law Review 939 (2000).

[6] See Benkler, *Rules of the Road for the Information Superhighway: Electronic Communication and the Law* '27.61(1)(f)(1996).

[7] *Ibid*.

[8] Kashi, *How to Conduct Electronic Media Discovery*, 7 The Practical Litigator 75, 78 (Nov. 1996).

[9] In the past, parties informally, or by court order, worked out an arrangement of the economical exchange of computer generated information. The information that exists on a computerized form should be produced in a format that is computer readable to all parties involved in the litigation. Where that has not been the case, courts have imposed court orders and related costs for the generating or producing party to assist the receiving party with the interpretation of the materials. *See Timken Co. v United States*, 659 F.Supp. 239, 243 (CIT 1987) [discovering party paid data service to determine how computer program functioned]. Under the newly amended FRCP, ESI management becomes part of a party's pre-trial conference obligations.

[10] At the heart of any electronic discovery analysis is *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309, 311 (S.D.N.Y 2003) ("*Zubulake I*"). In this employment discrimination case, the court was faced with plaintiff/employee's legitimate discovery requesting electronic documents, including deleted e-mails which could be found only on back-up disks on the employer's network. (*Id*. at 318.) Defendants produced ninety-four e-mail documents that revealed what the court deemed a "sort of smoking gun": an e-mail suggesting that "Zubulake be fired 'ASAP' after her EEOC charge was filed, in part so that she would not be eligible for year-end bonuses." (*Id.* at 312, fn.8.) Zubulake then sought production of defendants' active user e-mail files, archived e-mails on optical disks and backup data stored on tapes. (*Id.* at 320.)

[11] According to "*Zubulake I*, regarding whether electronic data is "accessible" or "inaccessible," the distinction "turns largely on the media on which it is stored." *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309, 318 (S.D.N.Y 2003). In order of descending accessibility, the categories of electronic data are (1) active, online data (hard drives), (2) near-line data (disks, magnetic tape, optical disks), (3) offline storage/archives (off-site archived data such as those "traditionally used for making disaster copies of records") (*Id.* at 319), (4) backup tapes and (5) erased, fragmented or damaged data." Of these categories, the first three are considered "accessible" in that the information that is stored is in a readily usable format. The last two categories are considered "inaccessible" because they involve data that was/is "not readily usable." According to the court, "backup tapes must be restored using a process similar to that previously described, fragmented data must be defragmented, and erased data must be reconstructed, all before the data is usable. That makes the data inaccessible." Backup tapes involve tape drives that have "different capabilities", run at "different transfer speeds", are "sequential-access devices" and also typically "employ some sort of data compression, permitting more data to be stored on each tape but also making restoration more time consuming and expensive, especially given the lack of uniform standard governing date compression." Erased, fragmented or damaged data entails even more difficulty in retrieval because once a file is erased, the contiguous clusters of stored information "are made available again as free space" and then newly created files may become larger than the remaining contiguous free space." *Id.* at 319. Both backup tapes and erased, fragmented or damaged data are far more costly to recover and produce in discovery. Thus, the distinction between "accessible" and "inaccessible" electronic discovery is critical.

[12] Imagine if this was allowed in the tobacco litigation or the asbestos related litigation of years past. Would damaging "smoking gun" corporate memorandums ever have seen the light of day or would they have been buried and hidden in "inaccessible" form by corporations in a purposeful effort to eliminate their production in litigation? The answer is obvious.

[13] In addition, the "not reasonably accessible" approach defined above could be construed differently than the "accessible" data under *Zubulake I*, discussed *supra*. *See Report of the Civil Rules Advisory Committee, in Report to Judicial Conference*, app.C (May 27, 2005) at 43-44.

Copyright © 2007 by the author.
For reprint permission, contact the publisher: **www.plaintiffmagazine.com**