A Primer on Electronic Discovery: What You Don't Know Can *Really* Hurt You

By Bradley C. Nahrstadt

Adapted from Bradley Nahrstadt's presentation at the 2008 FDLA Annual Meeting, this article provides a comprehensive introduction to the current state of electronic discovery.

No one can realistically argue that computers do not affect our everyday lives. Here are some sobering statistics about computers and the documents they generate:

- Somewhere between 93 and 97 percent of all information is now created electronically.
- It is commonly accepted that less than three percent of that information will ever be converted to paper.
- We are now sending more than 35 billion e-mail messages daily in the United States.
- More than 80% of corporate communications are sent via e-mail.
- Worldwide, we are sending more than 141 billion e-mails and producing one to two exabytes (the equivalent of one to two trillion books) per year.
- More than 50 % of the evidence that is produced today is in e-mail form.
- One CD holds the equivalent of 35,000 pages or 15 boxes of documents.
- The desktop or laptop hard drive for one employee can hold 1.5 million pages or 600 boxes of documents.
- One company server can hold 100 million pages or the equivalent of 43 semi-truck loads of documents.
- One mid-sized company typically has 1.625 billion pages of documents in its possession at any one time; enough to reach from the Earth to the moon.
- For the largest companies with 20,000 workers or more, 34% said employee e-mail has been subpoenaed in the past year.
- Sixty-two percent of the companies surveyed doubt that they can show their e-records are reliable and accurate.
- Ten percent of the corporate lawyers surveyed report that they have settled a case rather than incur the costs of electronic discovery.[1]

Undoubtedly, computers have changed the way we obtain information, the way we communicate, and the way we conduct business. They have also changed the way we conduct litigation. In light of the foregoing, it is vitally important for attorneys (and their clients) to understand the rules regarding electronic discovery, the nature and extent of electronic data, the means available to preserve that data at the beginning of a lawsuit, how such data should be requested, and the sanctions for failing to preserve

ABOUT THE AUTHOR...

BRADLEY C. NAHRSTADT is a partner with the Chicago, Illinois litigation firm of Williams Montgomery & John Ltd. He received his B.A., summa cum laude and with distinction from Monmouth College in 1989 and his J.D., cum laude, from the University of Illinois College of Law in 1992. He concentrates his practice on the defense of product liability, commercial and insurance bad faith matters. He is a member of the Board of Directors of the Illinois Association of Defense Trial Counsel.

electronic evidence. Each of these items will be addressed in turn.

The Rules Regarding Electronic Discovery

In 1970, Federal Rule of Civil Procedure 34 was amended to specifically provide for the discovery of electronic documents. In 2005, the federal judiciary's Civil Rules Advisory Committee adopted proposed changes to the federal rules dealing with electronic discovery. These proposed changes were subsequently approved by the Standing Committee on the Federal Rules of Civil Procedure and the U.S. Judicial Conference. On April 12, 2006, the proposed changes were approved by the U.S. Supreme Court. The amended rules took effect on December 1, 2006.

The amendments to F.R.C.P. 16 and F.R.C.P. 26 recognize the importance of locating and preserving electronic data at an early stage of the litigation. Rule 16 sets up a framework for the parties to address the "disclosure or discovery of electronically stored information," and to identify issues relating to privilege at the Rule 16 Scheduling Conference. Rule 26(b)(2)(B) addresses the distinction between accessible and inaccessible data and allows the court to shift the costs of producing inaccessible data to the responding party. The rule now states:

> A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(c). The court may specify conditions for the discovery.

F.R.C.P. 26(b)(2)(B). Rule 26(b)(5)(B) codifies the doctrine of inadvertent waiver of privilege. Rule 26(b)(5)(B) has been amended to read:

> If information is produced in discovery that is subject to a claim of privilege or of 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 specified information and any copies it has 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, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved.

F.R.C.P. 26(b)(5)(B).

It should be noted that a major revision to the Federal Rules of Evidence, which just recently took effect, also protects against the inadvertent waiver of the attorney-client privilege and work product protection. On September 19, 2008, President Bush signed into law S. 2450, a bill adding new Evidence Rule 502 to the Federal Rules of Evidence. Federal Rule of Evidence 502 states as follows:

Rule 502. Attorney-Client Privilege and Work Product; Limitations on Waiver

The following provisions apply, in the circumstances set out, to disclosure of a communication or information covered by the attorney-client privilege or work-product protection.

(a) DISCLOSURE MADE IN A FEDERAL PROCEEDING OR TO A FEDERAL OFFICE OR AGENCY; SCOPE OF A WAIVER.— When the disclosure is made in a Federal proceeding or to a Federal office or agency and waives the attorney-client privilege or work-product protection, the waiver extends to an undisclosed communication or information in a Federal or State proceeding only if:

(1) the waiver is intentional;

(2) the disclosed and undisclosed communications or information concern the same subject matter; and

(3) they ought in fairness to be considered together.

(b) INADVERTENT DISCLOSURE.— When made in a Federal proceeding or to a Federal office or agency, the disclosure does not operate as a waiver in a Federal or State proceeding if:

(1) the disclosure is inadvertent;

(2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and

(3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).

(c) DISCLOSURE MADE IN A STATE PROCEEDING.— When the disclosure is made in a State proceeding and is not the subject of a State-court order concerning waiver, the disclosure does not operate as a waiver in a Federal proceeding if the disclosure:

(1) would not be a waiver under this rule if it had been made in a Federal proceeding; or

(2) is not a waiver under the law of the State where the disclosure occurred.

(d) CONTROLLING EFFECT OF A COURT ORDER.—
A Federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court—in which event the disclosure is also not a waiver in any other Federal or State proceeding.

(e) CONTROLLING EFFECT OF A PARTY AGREEMENT.—
An agreement on the effect of disclosure in a Federal proceeding is binding only on the parties to the agreement, unless it is incorporated into a court order.

(f) CONTROLLING EFFECT OF THIS RULE.—
Notwithstanding Rules 101 and 1101, this rule applies to State proceedings and to Federal court-annexed and Federal court-mandated arbitration proceedings, in the circumstances set out in the rule. And notwithstanding Rule 501, this rule applies even if State law provides the rule of decision.

(g) DEFINITIONS.—
In this rule:

(1) 'attorney-client privilege' means the protection that applicable law provides for confidential attorney-client communications; and

(2) 'work-product protection' means the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial.

According to Rule 502, the new rule shall apply in all proceedings commenced after the date of enactment of the rule and, insofar as is just and practicable, in all proceedings pending on the date of enactment (September 19, 2008).

Rule 26(f) now requires the parties to discuss "any issues relating to preserving discoverable information," and "any issues relating to disclosure or discovery of electronically stored information, including the form in which it should be produced." Rule 26(f)(4) has been amended to require the parties to specifically discuss "any issues relating to claims of privilege or of protection of trial-preparation material, including—if the parties agree on a procedure to assert such claims after production—whether to ask the court to include their agreement in an order." This discussion between counsel is to take place at least 21 days before the Scheduling Conference is held or a Scheduling Order is submitted by the parties.

Rule 33 now states that where business records are stored in an electronic format, and the burden of answering an interrogatory is substantially the same for the party serving the interrogatory as for the party served, the responding party may simply identify the electronic data and allow the requesting party a reasonable opportunity for inspection and copying.

Rule 34(a) has been amended to allow a party to serve on any other party a request to produce any designated electronically stored information or any designated documents (including writings, drawings, graphs, charts, photographs, sound recordings, images and other data or data compilations in any medium). Amended Rule 34(a) also allows parties to request to sample any designated electronically stored information. Rule 34(b) has been amended to allow the responding party to designate the form in which it wants electronically stored information to be produced. The amended rule provides:

> ...If a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained, or in a form or forms that are reasonably usable.
>
> ...A party need not produce the same electronically stored information in more than one form.[2]

Rule 37(f) deals with the sanctions associated with a failure to preserve electronic data. Rule 37(f) provides:

> Electronically Stored Information. 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.[3]

Rule 45 acknowledges that electronic information can be sought through the use of a subpoena. Rule 45 has been amended to allow a party requesting documents to specify the form of production. Other amendments allow testing and sampling of electronic documents, objection to the form of production, protection from undue burden, provisions relating to the production of data that is not reasonably accessible and inadvertent waiver of privilege.

So far, almost one third of the individual states have adopted rules specifically dealing with electronic discovery. Some of the rules are exceptionally detailed and mirror the provisions set forth in the revised Federal Rules of Civil Procedure; other merely indicate that the production of documents includes documents stored in an electronic format. The states that have enacted electronic discovery rules, in some form or another, are: Arizona, Idaho, Indiana, Iowa, Louisiana, Maryland, Minnesota, Mississippi, Montana, Nebraska, New Hampshire, New Jersey, New

York, North Carolina, Texas and Utah.

Florida has not yet passed any rules specifically dealing with electronic discovery, although Rule 1.350 of the Florida Rules of Civil Procedure states that a party may request that any other party produce "...any documents, including writings, drawings, graphs, charts, photographs, phono-records, *and other data compilations from which information can be obtained [or] translated...*" This would undoubtedly include electronically stored information. And certain commentators have noted that the Florida Bar is currently considering amendments to the state discovery rules to address the issues associated with electronic discovery.[4]

Although Florida does not have specific rules regarding electronic discovery, there are resources available to the state trial judges (and the lawyers who appear in front of them) who are grappling with electronic discovery issues. In August of 2006, the Conference of Chief Justices adopted and published *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information.*[5] Although these guidelines are not intended to serve as model rules for the state courts, they are intended to help trial judges identify and effectively address electronic discovery issues. The guidelines define relevant terms and discuss topics such as early attention to electronic discovery issues, the scope of electronic discovery, the format of production, allocation of costs, inadvertent disclosure of privileged information, preservation orders and sanctions. Some state courts have already indicated a willingness to use the guidelines when deciding e-discovery issues.[6]

In a further effort to provide state trial judges with some guidance about electronic discovery issues, The National Conference of Commissioners on Uniform State Laws is also in the process of drafting a uniform, multi-jurisdictional set of electronic discovery guidelines. At this point, the proposed rules are in the drafting and public comment stage.[7] The Commissioners' rules are modeled on the federal rules, with one main difference: they leave the judges with a lot of discretion to determine which types of cases should be governed by the rules and allow the judges the option of exempting certain types of cases from their requirements.

Types of Discoverable E-Data

Electronic discovery ("e-discovery") is the process of requesting, obtaining, and reviewing material that has not been reduced to a tangible medium (such as paper or microfilm) or that co-exists with a tangible copy.[8] Common types of material include e-mail messages, voice mail messages, word processing files, spreadsheets, diaries, cell phone text messages, textbook information (including data from Personal Digital Assistants), Internet use histories, and files downloaded from the Internet.[9] Even though a party may have produced material in a tangible form, chances are the electronic version of that material will contain additional information, known as metadata. Metadata, which is defined as "information describing the history, tracking or management of an electronic document," can reveal revisions, deleted material, typist information, the document creation date, the author of the document, subsequent edit dates of the document, who accessed the document, and the number of versions of the document in existence. Although this information is held with the file in its native format, none of it is visible on the printed version of the document.[10]

Electronic data essentially falls into three general categories: data files, background information, and electronic mail. The data files consist of five general types of information that are processed and stored electronically: active data, archival data, back-up data, legacy data and residual data.[11] Active data is readily accessible and comes in many formats, such as word processing documents, spreadsheets, databases, e-mail messages, and electronic calendars. Active data files are accessed through programs such as File Manager and Explorer in the Microsoft Windows environment.[12]

Archival data is stored separately from active data because it is no longer in use by the computer. Some computer systems have automatic back-up systems, which create back-up data files while the user is creating a document. These archived files can be used to recreate a file should a malfunction occur. However, until the data is needed, it is archived and stored awaiting a request for delivery.

Back-up data is typically a snapshot of active data which has been copied to a storage medium, such as floppy discs, magnetic tapes, zip drives or CD-ROMs. Back-up data is a good source of historical information, as many businesses routinely use back-up procedures which can hold data going back years. Additionally, back-up data files are a good place to look for evidence, as many versions of a particular document may exist in this format.[13] The downside to the discovery of back-up data results from the ability of back-up storage media to hold incredibly large amounts of data. If the back-up data filing system is poorly organized, a great deal of time and expense will be required to sort through the information.[14]

Legacy data is the data that remains on laptop computers, desk top computers, servers and other electronic equipment that has been removed from active use. Off-the-shelf operating systems and application software commonly used by businesses, individuals and the government is updated and superseded at a dizzying pace. In a technological environment that is constantly changing, operating systems and application software become outdated and unusable after only a few years. Likewise, the physical media on which digital information is stored, and the hard-

Continued on page 25

Continued from page 20

ware needed to read and retrieve that information, are constantly changing to accommodate advances in technology.[15] Although systems, software and media are constantly updated, vast quantities of electronic information is not migrated to the new components. The data that remains on the old devices does not disappear—it is waiting to be discovered and produced. This legacy data can also be an excellent source of discoverable information.

Residual data still exists on hard drives and in the memory of printers and fax machines, even though the user attempted to "delete" the file. The files that are deleted by the user are merely marked by the computer as available space and the information will remain intact until other data or programs override the space.[16] Depending on the size and use of the computer system, it may take weeks or even months to override the space containing the "deleted" information.[17] Additionally, sometimes "deleted" files are only partially overwritten, which enables competent computer forensic experts to recover the remaining parts of the document.[18] Moreover, even if new files or programs use the space containing the "deleted" information, some of the "deleted" information will remain intact, and subject to discovery, if the new file or program is smaller in size than the deleted file.[19]

Not all data is recoverable. Some examples of unrecoverable data include data that was stored on a drive area that has been wiped clean, instant messages, overwritten files (although in certain instances some information can be recovered by a forensic computer expert), encrypted files, segments of files and files upon which "file shredding" applications have been run.

The second category of potential electronic evidence that may be waiting to be discovered in a case is the background information a computer system can create, such as audit trails, access control lists, and non-printing information. Audit trails contain information about who accessed the 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 that information.[20]

Access control lists are used to limit employee access to a company's computer system in such a way that the lists can describe who has access to particular information, thus allowing for increased ability to establish ownership or authenticity of the information.[21] Finally, non-printing information is data that exists as part of a file or document, but does not actually appear printed out on the face of the document. Non-printing information can include information which indicates when a document was created, modified or deleted, as well as notes or comments that users place in their documents when created with a program that allows a user to insert "hidden" comments in the text. These "hidden" comments do not become part of the printed version and, thus, are only available when accessed electronically.[22]

As noted above, this background information is known as metadata. It is the data about the electronic data or the data embedded in the file that gives details regarding the attributes of the file. Evidence can "hide" within the metadata of a file and, if relevant, should be requested in particular discovery requests. Metadata can include a file's:

- Creation time/date stamp – typically the time/date the file was put in that particular folder and particular location. The creation date changes every time a file is copied to another location.
- Access time/date stamp – The computer's time/date when the file was last touched by the operating system.
- Modification time/date stamp – The computer's time/date when the file was last modified.
- Author.
- Number of revisions.
- Time/date the file was last printed.

Electronic evidence can also "hide" in Enhanced Metafiles (EMF files – the graphic representation of a file that is sent to the printer when you print, usually written to the disk in a temporary directory), and Link Files (pointers to other files with metadata that contains information about the referenced file).[23]

A number of courts have recognized the evidentiary value metadata can offer and have routinely ordered parties to preserve metadata during the discovery process. In *Williams v. Sprint/ United Mgmt Co.*,[24] the court held that "when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with the metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order." A similar result was reached in the case of *In re Verisign, Inc. Sec. Litigation*.[25]

The last category of electronic evidence is electronic mail. E-mail is now among the most popular modes of communication in the work place. The characteristics of e-mail, combined with the number of e-mail messages traveling the data wires of businesses and households, makes it an excellent source for evidence in just about any type of case.[26] What most users do not realize is that e-mail is extremely difficult to erase and is more likely to be permanent than paper letters. The simple fact of the matter remains that simply using the delete key on the computer keyboard does not permanently erase an e-mail message. Moreover, if the author's (or recipient's) employer runs periodic back-ups of

their network, e-mail messages are "backed-up" and stored on back-up tapes, making the messages as long lasting as the tapes themselves.[27] In addition, because of the reply and forwarding features of most e-mail systems, e-mail messages can be sent to an unlimited number of users and receivers, thereby making the message even harder to truly delete when the need or desire arises.[28]

Because of a perception of privacy and a belief that e-mail messages are "easily destroyed," users often express frank thoughts and opinions in an e-mail message that they would not normally put in a formal memorandum or letter. One commentator has noted that, "most individuals have the false impression that e-mails are confidential, like telephone communications."[29] This same commentator has reported that some psychologists have observed that the computer creates an ease of communication that encourages the sender and the recipient to talk openly as if they were on a private stroll around the park.[30] The same is true for cell phone text messages, which, despite their transient impression, are capable of being saved by wireless companies on servers and retrieved from an archival system. This dangerous misconception that such information is privileged and capable of permanent deletion has led to the production of severely damaging evidence in a number of recent cases.

In *U.S. v. Microsoft Corp.*,[31] the Department of Justice accused Microsoft of anti-competitive practices, including improperly using its windows monopoly to achieve dominance in the Internet browser and e-commerce markets. The government's case-in-chief was supported by a number of damning e-mails written by Microsoft employees discussing precisely how Microsoft intended to obtain a monopoly on the Internet browser market. In *Strauss v. Microsoft Corp.*,[32] the court allowed the plaintiff to introduce into evidence certain e-mail messages created by the defendant's employees which contained inappropriate sexual and gender-related comments. The court admitted the e-mail messages on the grounds that they were directly relevant to the plaintiff's claim that she was discharged in retaliation for claiming that she was denied a promotion because of her gender. And in *Vermont Microsystems Inc. v. Autodesk, Inc.*,[33] the plaintiff was able to prevail on its trade secrets claim based on similarities between the parties' versions of computer-aided designed software. Electronic discovery in the case revealed that a former employee of the plaintiff had brought the trade secrets to the defendant. Specifically, the plaintiff's former employee sent an e-mail to his colleagues at the defendant corporation detailing the tactical specifications and overall architecture of the plaintiff's system and the defendant's system.

Requesting the Electronic Data Itself

It is impossible in an article such as this to set forth all (or even most) of the interrogatories and requests for production of documents that could be filed by counsel regarding the issue of electronic discovery. The requests themselves will be limited only by the creativity of counsel and the manner and number of claims filed.

That having been said, any interrogatories that are filed by counsel must contain requests for relevant electronic information concerning each and every one of the plaintiff's claims. At the very least, information should be sought from all of the sources of electronic discovery identified in the initial discovery requests regarding operating systems, hardware, software, and loose media.

Counsel should keep in mind that Rule 33(a) of the Federal Rules of Civil Procedure (and many state court discovery rules) limits the number of interrogatories that a party can propound to the other side. As such, it may be necessary for counsel to obtain an agreement or stipulation for the other side to issue more extensive interrogatories designed to obtain relevant information about how the opposing party generates, reviews, retains, stores and destroys its electronic evidence.

Once counsel has a general sense of her opponent's technological infrastructure, she should be in a position to draft appropriate requests for the production of electronically stored information. Typically, counsel will be looking for information in three basic areas: e-mail, electronic documents and data compilations. Not every case will require discovery in all three areas, but counsel should stop and consider whether electronic information exists in all three areas when framing her requests.[34] There are some general considerations that should be kept in mind when preparing requests for the production of electronic evidence. Counsel must determine whether to request information in native format and, if so, whether there is certain metadata that does not need to be included in the production. If certain metadata is not required, counsel should indicate that on the face of the requests in order to expedite the process of producing the information and limit the expense associated with reviewing it once it is produced. If counsel does not want the information produced in native format, careful thought must be given to the format to be used for the production. For example, if only images are to be requested, does counsel want TIFFs, PDFs or something else?[35]

If counsel intends to use some type of litigation support software to review the production responses (such as Summation or Concordance), counsel will generally want documents produced in native format and to have the metadata included (or at least the metadata that these programs are capable of displaying). Counsel must recognize that if he does not ask for the information to be produced in native format, and accepts the initial

production as an image file, the potential for uncovering the available metadata will be lost.[36]

Finally, when dealing with requests for e-mail, counsel must be sure to request not only all related metadata, but also all attachment files. This is one area in particular where metadata is particularly important, not only substantively, but in terms of using litigation support technology to successfully manage the information. As one set of commentators has noted, "counsel needs to know how to ask for this information in a way that will work successfully with the tools that are available to process it."[37]

Drafting electronic discovery requests can be a tedious and time consuming process. But it is necessary in order to uncover not only the location of electronic documents, but also the actual electronic data itself that can be used to prosecute the claim or prevail on the defense.

Preserving Electronic Information Prior to Discovery

Because electronically stored information is subject to deletion at any time, and because such deleted information is subject to being overwritten at any time, there is an overriding need to act quickly early in the litigation to conduct discovery regarding electronically stored data.[38] Although there is a need for speed in obtaining information regarding electronically stored data, standard discovery procedures are not geared toward such immediate action. The Federal Rules of Civil Procedure, and most state rules of procedure, impose time restrictions on when discovery can be initiated and allow parties specific periods of time after the receipt of discovery (usually 30 days) to respond to the same. An enormous amount of electronic data can be destroyed or lost during such time frames.

There are essentially three procedures that can be employed in an effort to protect the purposeful or inadvertent destruction of electronic data: *ex parte* seizure orders, protective orders, and written requests for preservation of electronic evidence.

A. *Ex Parte* Seizure Orders

Ex parte seizure orders can be granted and executed before a party is even aware of a lawsuit. The fact that the court will order the seizure of computer-related information before a party has received notice of the lawsuit prevents the party from concealing or destroying evidence. However, the power of the court to seize a party's property without notice and an opportunity to be heard is strictly limited by either rule or statute and, understandably, the mandates of the United States Constitution.[39] Statutes and rules to consider for *ex parte* authority to engage in a seizure of electronic information or computer equipment include Rule 65 of the Federal Rules of Civil Procedure, the Trademark Counterfeiting Act of 1984, and the U.S. Copyright Act.[40]

B. Temporary Restraining or Protective Orders

The second option is to obtain either a temporary restraining order or a protective order from the court. These types of orders, which are issued after notice to the opposing side, would require the party against whom the order is entered to preserve the information identified in the application for the temporary restraining order or protective order. Since maintaining computer records is generally less onerous than requiring companies to maintain warehouses full of documents, courts have not been hesitant to enter preservation orders.[41]

C. Litigation Hold Letters

The final option, a written request for the preservation of electronic evidence (also known as a litigation hold letter), was addressed in minute detail in a series of opinions authored by Judge Shira Scheindlin, a district court judge in the Southern District of New York. In 2003, Judge Scheindlin began authoring a series of opinions known as the *Zubulake* opinions, all of which are a must read for any lawyer who is engaged in electronic discovery. The fourth and fifth *Zubulake* opinions contain a detailed discussion of the litigation hold, its role in today's litigation, and the lawyer's obligation to issue the litigation hold and then follow up.[42]

1. Preserving Your Opponent's Data

According to Judge Scheindlin, the obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation. While a litigant is under no duty to keep or retain every document in its possession, it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.

Judge Scheindlin recognized in *Zubulake IV* that, in light of the "many ways to manage electronic data," there will often be a variety of options for a litigant once the duty to preserve data attaches:

> The scope of a party's preservation obligation can be described as follows: Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents. As a general rule, that litigation hold does not apply to inaccessible back-up tapes (*e.g.*, those typically maintained solely for the purpose of disas-

ter recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if back-up tapes are accessible (*i.e.*, actively used for information retrieval), then such tapes *would* likely be subject to the litigation hold.

However, it does make sense to create one exception to this general rule. If a company can identify where particular employee documents are stored on back-up tapes, then the tapes storing the documents of "key players" to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available. This exception applies to *all* back-up tapes.[43]

So how does counsel guarantee that the duty to preserve is triggered? By sending the opposing side a litigation hold letter. The litigation hold letter sent to the opposing party should explain that all relevant electronic data must be preserved and safeguarded from destruction. The litigation hold letter to the opposing party should also identify, as specifically as possible, the information to be preserved and warn of the possible consequences for the destruction of relevant electronic data.

2. Preserving Your Own Client's Data

The preservation obligation runs both ways. If counsel does not follow the steps outlined below and issue a litigation hold to her own client, the sanctions discussed at the beginning of this article may become an all too real possibility.

The first thing counsel must do when faced with the prospect of litigation is to become fully familiar with the client's document retention policies, as well as the client's document retention architecture. Counsel should first obtain a copy of the client's document retention policy, if it has one. The policy should be reviewed for what it does and does not cover and special attention should be paid to electronic data. Counsel should also find out if any litigation holds have been issued since the document retention policy was put in place. Key employees of the client should be interviewed to see what went right and went wrong with the prior litigation hold. Every effort should be made to identify whether there were employees who refused to follow the litigation hold, difficulties with the technology, cost overruns, or other issues.

Counsel will have to sit down with the major business units that will be affected by the litigation hold. Departmental managers, company executives, human resources personnel and the head of the company's Information Technology department will need to explain how data is created, how it is stored, how it is retained and how it is destroyed. Particular attention should be paid to interviewing the IT personnel. Counsel should ask the IT personnel to explain, in the simplest terms possible, how information is processed through their system. Send the IT department an e-mail and ask the personnel to explain exactly how that e-mail flows through the company's system. Ask to see the servers that the electronic data is stored on, the back-up tapes that are used to copy the electronic data and the off-site storage facilities where data is kept in case of disaster.[44] Counsel should also ask if the company has a formal policy on computer use, find out the computer rights of all data custodians and what sort of hardware turnover the company has had during the period relevant to the suit. Once the storage points are identified, counsel should inquire how long electronic evidence will reside on each particular tape, server, CD-ROM, hard drive, etc. Every effort must be made to understand the intricacies of the system and how electronic evidence is created, processed, categorized, stored and deleted.[45]

It cannot be stressed enough that counsel and the IT personnel must be on the same page when it comes to the preservation and production of electronic data. Counsel must fully understand what is requested and question how the IT personnel will go about meeting the request. For example, suppose counsel requests a "mirror image backup" of an employee's hard drive. Counsel's intention is to have an exact copy (a mirror image) of the hard drive made in order to ensure the integrity of the data—but that intention is never communicated to the IT personnel who are working on the project. Instead of making a mirror image copy of the hard drive, the IT personnel preserve the data by placing it on backup tape media. When the technicians heard "backup," they assumed the attorney meant a backup tape. Since backup tapes can be difficult to read, the actions of the IT personnel will inevitably increase the costs of extracting and producing the responsive date and could lead to claims that counsel was trying to hide evidence on an inaccessible media.[46]

Or suppose that counsel notifies the IT department to preserve the company's e-mails and other electronic data for a legal matter. The IT department, having received no input from counsel, copies the native files to an external hard disk drive (thus changing the metadata), places the company's e-mails and databases on backup tapes (making the data inaccessible) and fails to segregate and protect the original data. As a result of this miscommunication and lack of understanding, the preserved data resides on separate media formats, increasing the search and retrieval costs, and the original data is still exposed to change or deletion.[47]

Neither of these scenarios is beyond the realm of possibility. In fact, both are most likely prob-

abilities if each side doesn't take the time to understand the issues and carefully communicate what is requested and what is required of all parties involved in the electronic discovery process.

During these important conversations, counsel must meet with all employees who will be directly involved in the litigation, as well as the IT personnel, in order to learn what electronic data is germane to the case and where it is stored. Employees directly involved in the case should be interviewed about their technology patterns and habits. E-mails, word processing documents, spreadsheets, data compilations, instant messages and voice mails must be identified so that steps can be taken to make sure that the evidence is properly preserved. This may also require changing IT policy and procedures such as overwriting back-up tapes or an auto-delete function in e-mail. As one commentator has noted, "[e]xecuting effective, reasonable and direct communication with every [source and custodian of relevant information] minimizes risk, eliminates miscommunications and resolves perceptions of due diligence neglect."[48]

As part of this process, counsel must communicate directly with the "key players" in the litigation. The key players would be those people identified in the party's initial disclosures, initial pleadings and any subsequent supplementations or amendments to those documents. Some examples of key players may include Human Resources personnel (who may have information about former employees as potential sources of information), Records Management personnel (who will have to be instructed to suspend normal destruction procedures and preserve relevant documents) and Information Technology personnel (who will be intimately involved in the identification and recovery of electronic data).[49] Key players can and should also be identified by internal witness interviews conducted in anticipation of litigation or at the start of the case.[50] Because the key players are the employees who are most likely to have relevant information about the case, it is particularly important that the duty to preserve electronic evidence be communicated clearly and directly to them at the earliest possible stage in the litigation.[51]

At the very outset of the litigation, counsel must issue a litigation hold letter to ensure the preservation of relevant data. This letter must explain to all the employees of the company who have possession of relevant electronic data that the data must be preserved and safeguarded from destruction. The litigation hold letter should identify, as specifically as posible, the information to be preserved. As one commentator has noted, the litigation hold letter "...consists of a written directive to all potentially relevant personnel of a company advising them that there is a specific subject matter which has resulted or is likely to result in litigation, to describe that subject matter, and the people involved in it, in sufficient degree to inform the recipients of this communication of the true nature of the actual or anticipated dispute, and then to specifically advise them to both locate and save all relevant paper documents, e-mails, and any other items that may be contained in the company's computer system."[52] In addition, all employees must be told that any document destruction policy in place at the company must be suspended and that the employees are not to delete anything pertinent to the case, be it an existing document or e-mail or data created after the date of the preservation letter. The client's employees should also be provided with an explanation of the serious nature of the litigation hold and the penalties that may be imposed upon the company if electronic data is unintentionally, or intentionally, destroyed.

In summary, the litigation hold letter should spell out, in plain English, the responsibilities of each employee, convey the specifics on documents and information required to be preserved, impart unique responsibilities based on each employee's role in the litigation and their function within the company:

- Describe the background of the case and how long it is expected to last;
- Identify information subject to preservation (paper and electronic);
- Specify pertinent data types and their associated applications, electronic and paper document preservation and retention methods, and preservation tools and how to use them;
- Inform employees of their legal obligations, including the ramifications and penalties for non-compliance with the litigation hold.[53]

In addition to containing the information outlined above, the litigation hold letter should provide contact information in case the recipient of the letter has any questions or requires assistance. More than likely, two points of contact should be included in the letter: an attorney contact for the legal and subject-matter issues and a technical contact to assist with hardware or software issues. Most importantly, the litigation hold letter must be reissued periodically to all employees who may have relevant information in their possession in order to remind them of their preservation obligations and duties. The litigation hold letter most certainly must be reissued if the issues or key players in the case change.[54]

It is important to remember that, according to some courts, the duty to ensure the preservation and production of all relevant electronic documents rests ***with counsel***. Judge Schiendlin noted several examples of this duty in *Zubulake V*:

> A party's discovery obligations do not end with the

implementation of a "litigation hold" — to the contrary, that's only the beginning. **Counsel** must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce relevant documents. [...]

Once a "litigation hold" is in place, a party and her counsel must make certain that all sources of potentially relevant information are identified and placed "on hold," to the extent required in *Zubulake IV*. To do this, counsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture. This will invariably involve speaking with information technology personnel, who can explain system-wide back-up procedures and the actual (as opposed to theoretical) implementation of the firm's recycling policy. It will also involve communicating with the "key players" in the litigation in order to understand how they stored information.

* * *

To the extent that it may not be feasible for counsel to speak with every key player, given the size of a company or the scope of the lawsuit, counsel must be more creative. It may be possible to run a system-wide keyword search; counsel could then preserve a copy of each "hit."

* * *

In short, it is *not* sufficient to notify all employees of a litigation hold and expect that the party will retain and produce all relevant information. Counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched.

Once a party and her counsel have identified all the sources of potentially relevant information, they are under a duty to retain that information (as per *Zubulake IV*) and to produce information responsive to the opposing party's request. Rule 26 creates a "duty to supplement" those responses. Although the Rule 26 duty to supplement is nominally the party's, it really falls on counsel.[55]

After this pronouncement, the court went on to note that there are a number of steps that counsel must take to ensure compliance with the preservation obligation. First, counsel must issue a litigation hold at the outset of the litigation or whenever litigation is reasonably anticipated. That hold should be periodically re-issued so that new employees are aware of it and so that it is fresh in the minds of all employees. Second, counsel should communicate directly with the "key players" in the litigation, i.e., the people identified in a party's initial disclosures and any supplementation thereto. Because the "key players" are the employees likely to have relevant information, it is particularly important that the preservation duty be communicated clearly to them. The "key players" should be periodically reminded that the preservation duty is still in place. Finally, counsel should instruct all employees to produce electronic copies of their relevant active files.

Given this warning, it is vitally important that counsel oversee compliance and monitor efforts to comply with the litigation hold and produce responsive documents to the other side. Perform periodic checks of your client's system to make sure documents are not being destroyed or altered. Set up special programs in order to collect and store electronic data. Meet frequently with the key players to ascertain that they are following the directives set forth in the litigation hold letter.

Finally, if you have done all of the above, do not let it go to waste. Remember to document your efforts to implement and monitor the litigation hold. Create memoranda that identify the persons with whom you spoke, the topics that were discussed, the materials that were provided to each key player or data custodian and the documents that were produced and/or collected from each person. And make sure that you keep all this data in one centralized location in the event that you need to rely on it to show that you complied with the letter and the spirit of the law.[56]
In short, counsel must be able to demonstrate that he or she, and the client, were committed to "good faith" preservation efforts.

- Send key players periodic reminders of their obligations;
- Inform employees of additional responsibilities as the scope of the action changes;
- Institute tracking and audit capabilities;
- Retain the messages or notifications sent to employees describing their legal obligations and responsibilities; and
- Assess whether relevant personnel should be required to certify their preservation and retention actions.[57]

A major part of being able to demonstrate good faith preservation efforts is education. In order to accomplish the goals set forth above, companies would be well advised to begin educating their

employees about the nature and extent of litigation holds—even before a hold needs to be put in place. Companies should begin the process of indoctrinating their employees on their preservation and retention responsibilities, providing periodic refresher training and mandatory seminars on new or revised legal requirements. Key departments, including Records, Legal, HR and IT must be trained regarding the company's legal hold policies and their exclusive preservation and compliance responsibilities.[58]

To summarize, the relevant case law indicates that counsel must do the following when it comes to implementing a proper litigation hold:

1. Become familiar with the client's document retention and destruction policies and computing infrastructure, speaking with the client's key IT personnel in order to do so. Ensure that the IT personnel not only preserve data but also verify that they have suspended any and all automated processes which could inadvertently destroy information until the data is collected and determined to be irrelevant.

2. Learn how information is created, maintained and destroyed, identify and account for accessible and inaccessible electronically stored information and confer with IT personnel to devise cost effective and valid methods of data collection.

3. Communicate directly with all key players involved in the litigation, inquiring as to how and where they store their information and advising them of their preservation obligations. Provide the key players with the complete picture. Explain in plain English the circumstances of the matter, the facts in dispute, the types of relevant information (e-mails, spreadsheets, etc.), internal and external points-of-contact and potential repercussions for non-compliance.

4. Ensure that a litigation hold is implemented whenever litigation is reasonably anticipated and periodically reissue the litigation hold.

5. Instruct all employees to produce responsive electronic and paper documents and files and ensure that relevant back-up tapes and other archival material are safely stored away.

6. Actively monitor compliance so that all sources of discoverable material are identified and searched, since it is not sufficient to advise the client of a litigation hold and then expect the client to retain, identify and produce the relevant evidence. Verify that all key players are notified of, understand and acknowledge their preservation obligations.

7. Implement "forensically sound" methods of collecting responsive data.[59]

Sanctions for Spoliation of Electronic Evidence

In the movie "Jaws," Matt Hooper had the following response to Mayor Vaughn's denial that Amity had a shark problem: "I think that I am familiar with the fact that you are going to ignore this particular problem until it swims up and bites you on the ass." This quote seems to sum up the mindset of a large number of corporate executives and lawyers involved in complex litigation. The prevailing attitude seems to be "let's close our eyes and send a wish toward heaven that no one will ask for any electronically stored or generated evidence." But the days of hoping the problem will go away or that no one will think to ask for electronic discovery are long gone—especially in light of the revisions to the Federal Rules of Civil Procedure which now make requesting and producing electronic data an integral part of the discovery process.

More and more, the courts are taking an active role in policing the production of electronic discovery and are sanctioning those parties that have insisted on taking an "ignorance is bliss" attitude. In the last few years, there have been dozens of cases involving sanctions for the spoliation of electronic evidence. A review of just a handful from the last four years paints a very sobering picture of the actions courts will take to punish parties that are guilty of spoliation which occurred in the absence of—or even in the presence of—a litigation hold letter.

In *Zubulake v. UBS Warburg LLC,*[60] an employment discrimination case, the trial judge concluded that UBS acted willfully in destroying potentially relevant information, including e-mails about the plaintiff and her performance which resulted either in the absence of such information or its tardy production. As a result, she ordered that the jury empanelled to hear the case would be given an adverse inference instruction concerning the deleted e-mails at the time of trial. She further ordered that UBS was required to pay all costs associated with re-deposing any witnesses identified by plaintiff and to pay all costs associated with plaintiff's motion for sanctions. The *Zubulake* case went to trial in April of 2005. The trial judge stayed true to her word and the jury was given an adverse inference instruction. The jury returned a verdict in favor of the plaintiff and against the defendant for more than $29,000,000.

In *Coleman (Parent) Holdings Inc. v. Morgan Stanley & Co.,*[61] a Florida court issued an adverse inference instruction against Morgan Stanley for overwriting e-mails, failing to timely process hundreds of back-up tapes, and failing to produce relevant e-mails and their attachments. Relying in large part

on that instruction, the jury returned a $1.45 billion award against Morgan Stanley (a vedict that was later reversed on other grounds).

In *Arndt v. First Union National Bank*,[62] a dispute involving a contract made between the defendants and the plaintiff, the jury awarded the plaintiff over $830,000 in damages, relying in part on a spoliation instruction.[63] Although the plaintiff had requested various e-mails and profit and loss statements relating to the allegations, the defendant failed to preserve and produce these documents. The defendants argued on appeal that the instruction was unfairly prejudicial. The appellate court noted that testimony from one of the defendants' employees indicated that the defendants were on notice early on of the plaintiff's intention to sue the defendant but failed to preserve the plaintiff's e-mails or hard drive. The employee further testified that no effort was made to save the hard drive even after receiving a letter from the plaintiff's counsel about the case. Based on this evidence, the appellate court determined the trial court did not err in giving the spoliation instruction.

A review of recent cases paints a sobering picture of judicial responses to spoliation of electronic evidence...

In *Broccoli v. Echostar Communications Corp.*,[64] the plaintiff filed a motion for sanctions against the defendants for failing to preserve electronic documents and for destroying e-mails. The evidence showed that the defendants were on notice of the lawsuit long before they halted their data destruction policy. The defendants admitted they never issued a company-wide suspension of their data destruction policy and they did not save e-mails regarding the plaintiff's harassment. The court declared that the defendants acted in bad faith and issued an adverse inference instruction relating to the spoliation of the e-mails.

In *Tantivy Communications, Inc. v. Lucent Technologies Inc.*,[65] a patent infringement case, the plaintiff sought to exclude evidence based on the defendant's pernicious discovery abuse. During discovery, the plaintiff had sought documents contained on the defendant's Internet web site specifically relating to interoperability testing for the products at issue. The defendant had repeatedly represented that it was unaware of any such documents. However, one of the defendant's employees revealed at a deposition that, pursuant to the defendant's document destruction practices, paper documents were shredded and electronic documents were deleted that included interoperability contracts and test plans. Citing *Zubulake*, the court stated, "[the defendant] and its counsel are well aware that a party in litigation must suspend its routine document retention/destruction policy and establish a 'litigation hold' to ensure the preservation of relevant documents." The court further declared it would not allow "lawyers or their clients to lay behind the log and disregard their discovery obligations."

In *Paramount Pictures Corp. v. Davis*,[66] the plaintiff alleged that the defendant infringed upon the plaintiff's motion picture copyright. After uncovering the defendant's alleged activities by tracing his Internet protocol address, the plaintiff was granted access to defendant's computer and hired a forensic computer expert to conduct the examination. The expert determined that the defendant had wiped all the data off his hard drive and reinstalled the operating system—just 16 days after he received notice of the lawsuit. The expert was unable to determine whether plaintiff's movie had been on the computer prior to the investigation. Although the court indicated that an adverse inference instruction would be warranted, it did not issue one because the case was not being tried to a jury. Instead, the court noted that it would take the defendant's "willful destruction of evidence into consideration at the time of trial."

In *Sony Computer Entertainment Am., Inc. v. Filipiak*,[67] the plaintiff sought injunctive relief and damages from the defendant, claiming that he sold products that allowed users to play illegal copies of the plaintiff's PlayStation video games. The defendant agreed to an injunction prohibiting the marketing, sale and distribution of his products, and then continued to sell them. After confronting the defendant about his violation of the injunction, the parties agreed to execute a consent judgment for an amount to be determined following the completion of discovery. During discovery the defendant's hard drive was examined by a forensic expert and he determined that thousands of files, including sales files, had been deleted from the defendant's hard drive just days before it was produced for inspection. The court found that the defendant intentionally and in bad faith violated the terms of the consent judgment, as well as his discovery obligations under Rule 26, and awarded the plaintiff more than $6 million in damages.

DaimlerChrysler Motors v. Bill Davis Racing, Inc.[68] was a breach of contract action in which the plaintiff sought sanctions against the defendant for destroying relevant e-mails. The defendant claimed that its computer system was set up to delete both internal and external e-mails automatically, unless affirmative efforts were taken to preserve them. One of the defendant's key employees testified that he was never instructed to preserve relevant communications, even after the lawsuit commenced. The magistrate judge assigned to hear the dispute declared that "... normal procedures for destruction of documents must...be suspended

when a party is on notice that they may be relevant to litigation..." and recommended that the trial court issue an adverse inference instruction and an order allowing the plaintiff to present evidence of the spoliation.

In *Samsung Electronics. Co. v. Rambus, Inc.*,[69] a patent-infringement case, the court found that the defendant had implemented a document retention policy to justify destroying documents relevant to patent infringement claims when the defendant anticipated, or reasonably should have anticipated, litigation with the plaintiff. The court found the defendant's vague litigation hold instruction to "not destroy relevant documents" did not satisfy preservation obligations in light of several factors, including: the large volume of documents destroyed, the extent and kind of evidence destroyed following the hold, the failure of the instruction to specify which documents were relevant to litigation, and the fact that the defendant had maintained no records of the documents that were destroyed. In addition, the court offered guidance on how companies can comply with their preservation duties by modifying document retention policies already in existence. The court instructed companies to inform its officers and employees of pending litigation and identify for them the kinds of documents considered relevant, in addition to collecting and segregating relevant documents. The court observed a company simply cannot "make a document retention program an integral part of its litigation strategy and, pursuant thereto, target for destruction documents that are discoverable in litigation."

In re September 11th Liability Insurance Coverage Cases[70] dealt with coverage issues that arose following the September 11, 2001 attack on the World Trade Center. In the aftermath of the disaster, multiple suits were brought seeking insurance coverage on behalf of several of the entities that claimed an ownership or leasing interest in the complex. There were an enormous amount of documents produced by both sides. However, counsel for Zurich American Insurance Company failed to produce documents from the company's underwriting files in a timely fashion, allowed key electronic documents to be deleted, failed to produce paper versions of some of the deleted electronic documents until ordered by the court to do so and failed to ensure that a litigation hold was put in place and followed. The court noted that, "Discovery is run largely by attorneys, and the court and the judicial process depend upon honesty and fair dealing among attorneys." The court found that the actions of the defendant—**and its counsel**—violated F.R.C.P. 37 and imposed monetary sanctions of $500,000 on both the defendant and its counsel.

In *Southern New England Telephone Co. v. Global NAPs, Inc.*,[71] the plaintiff alleged that Global misrouted long-distance telephone traffic to certain circuits not designated for such traffic, thereby depriving SNET of applicable access charges. There was a two-year discovery battle over Global's financial records. During the course of discovery the plaintiff uncovered evidence that the defendant failed to produce electronic evidence when it claimed that the computer of a key witness "crashed." The "crash" was actually a purposeful dropping of the computer on the floor. The "crash" occurred **after** the court-ordered deadline for production of documents had come and gone. Discovery further revealed that the employee who dropped her computer used a program called Window Washer to delete and write over the information on her hard drive. The court found that the defendant committed a fraud on the court and that its willful discovery violations likely destroyed the plaintiff's ability to prove its case. The court entered a default judgment against the defendant in the amount of $5,247,781.45. The court also awarded fees and costs in the amount of $645,760.

In light of these opinions, and dozens more like them, it is vitally important that you take the issue of electronic discovery seriously and follow the steps outlined above (and in other places in this article) to ensure that spoliation of evidence does not become an issue in your case.

Electronic discovery, when appropriately tailored, can be a powerful discovery tool that can uncover a wealth of information to assist in prosecuting and defending cases in virtually every area of the law. On the other hand, electronic discovery can be expensive, onerous and time consuming for all parties, especially the responding party. Moreover, failure to comply with requests for electronic discovery can result in the imposition of substantial and even case-ruining sanctions. All attorneys practicing today should have a working knowledge of how to propound and respond to electronic discovery requests, since, as information technology continues to advance and its use becomes more pervasive, electronic discovery will no doubt play a critical role in litigation for many years to come.

1 Sharon D. Nelson, Bruce A. Olson and John W. Simek, *The Electronic Evidence and Discovery Handbook*, ABA Law Practice Management Section (April 2006), pp. xv-xvi; Jerry Crimmins, "E-mail at Big Biz Often Sought in Discovery, Survey Finds," Chicago Daily Law Bulletin, p. 1 (May 27, 2008).

2 F.R.C.P. 34(b)(ii) and (iii).

3 F.R.C.P. 37(f)(emphasis added).

4 Amy Karan and Kansas Gooden, "What to Do Without Local E-Discovery Rules," Daily Business Review (March 19, 2008).

5 A copy of the guidelines can be found at http://www.ncsconline.org.

6 *See, e.g., Analog Devices, Inc. v. Michalski*, 2006 WL 3287382 (N.C. Super. 2006) (unpublished opinion).

7 A copy of the current version of the proposed uniform rules can be found at http://www.nccusl.com.

8 Conrad J. Jacoby, "Electronic Discovery Requests," For the Defense, p. 39 (December 2001).

9 *Id.*

10 *Id.*

11 Devin Murphy, "Electronic Commerce in the 21st Century: The Discovery of Electronic Data in Litigation: What Practitioners and Their Clients Need to Know," 27 Wm. Mitchell L. Rev. 1825 (2001).

12 *Id.* at 1828.
13 *Id.*
14 *Id.* at 1828-1829.
15 Kenneth J. Withers, "Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure," Northwestern Journal of Technology and Intellectual Property, Vol. 4, No. 2, p. 175 (Spring 2006).
16 Murphy, *supra* note 9, at 1829.
17 Carey Sirota Meyer and Kari L. Wraspir, "E-Discovery: Preparing Clients For (And Protecting Them Against) Discovery in the Electronic Information Age," 27 Wm. Mitchell L. Rev. 939, 948 (2000).
18 *Id.*
19 Murphy, *supra* note 9, at1829.
20 *Id.*
21 *Id.* at 1830.
22 *Id.*
23 Ross L. Kodner, "Reliable Roadmap: The Solo/Small Firm Electronic Discovery Plan" (PowerPoint presentation, ABA Tech Show, 2006).
24 *Williams v. Sprint/United Mgmt Co.,* 2005 WL 2401626 (D. Kan. Sept. 29, 2005).
25 *In re Verisign, Inc. Sec. Litigation*, 2004 WL 2445243.
26 Murphy, *supra* note 9, at 1829.
27 Meyer and Wraspir, *supra* note 15, at 949.
28 Murphy, *supra* note 9, at 1829.
29 R. Mark Halligan, "The Brave New World of Electronic Evidence Discovery," 92 Ill. B.J. 296, 297 (June 2004).
30 *Id.* at 298.
31 *U.S. v. Microsoft Corp.*, 1998 WL 61485 (D.D.C. 1998).
32 *Strauss v. Microsoft Corp.*, 1995 WL 326492 (S.D. N.Y. 1995).
33 *Vermont Microsystems, Inc. v. Autodesk. Inc.*, 88 F.3d 142 (2d Cir. 1996).
34 Nelson *et al., supra* note 1, at 136.
35 *Id.*
36 *Id.*
37 *Id.* at 137.
38 Mark D. Robins, "Computers and the Discovery of Evidence—A New Dimension to Civil Procedure," 17 J. Marshall J. Computer and Info. L. 411, 485-486 (Winter 1999).
39 *Id.* at 487.
40 Murphy, *supra* note 9, at 1836.
41 *See United States v. International Business Machines Corp.*, 58 F.R.D. 556 (S.D.N.Y. 1973).
42 *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003) and *Zubulake v. UBS Warburg LLC,* 2004 WL 1620866 (S.D.N.Y. July 20, 2004).
43 *Zubulake IV,* 220 F.R.D. at 218 (emphasis added).
44 Stacy O'Neil Jackson, "Best Practices: Managing Litigation Holds in the Face of New Compliance Duties," Digital Discovery & e-Evidence, Vol. 5, No. 12, p. 2 (December 2005).
45 *Id.*
46 Neil R. Packard, "Understand Legal Hold Notification Changes," *E-Discovery Advisor*, Issue 6, p. 18 (2006).
47 *Id.*
48 *Id.* at 15.
49 *Id.* at 16.
50 Timothy J. Hogan, "The International and Domestic Implications of Electronic Discovery on Litigation and Business Practices," International Legal News, Vol. 2, p. 8 (June 10, 2005).
51 *Id.*
52 *Id.* at 7.
53 Packard, *supra* note 44, at 16.
54 Jackson, *supra* note 42, at 2.
55 *Zubulake*, 2004 WL 1620866 at *7-8 (S.D.N.Y. July 20, 2004) (emphasis added).
56 Jackson, *supra* note 42, at 3.
57 Packard, *supra* note 44, at 16.
58 *Id.* at 17.
59 Nelson *et al., supra* note 1, at 68-69; Packard, *supra* note 44.
60 *Zubulake v. UBS Warburg LLC,* 2004 WL 1620866 (S.D.N.Y. July 20, 2004).
61 *Coleman (Parent) Holdings Inc. v. Morgan Stanley & Co., Inc.,* 2005 WL 679071 (Fla. 15th Cir. Ct. 2005) (reversed on other grounds).
62 *Arndt v. First Union Nat'l Bank,* 613 S.E.2d 274 (N.C. Ct. App. 2005).
63 The trial court instructed the jury as follows: "[e]vidence has been received that tends to show that certain profit and loss statements and E-mails were in the exclusive possession of the defendant...and, [sic] have not been produced for inspection....From this, you may infer, though you are not compelled to do so, that the profit and loss statements and the E-mails would be damaging to the defendant."
64 *Broccoli v. Echostar Communications Corp.,* 229 F.R.D. 506 (D. Md. 2005).
65 *Tantivy Communications, Inc. v. Lucent Techs. Inc.*, 2005 WL 2860976 (E.D.Tex. Nov. 1, 2005.).
66 *Paramount Pictures Corp. v. Davis*, 2005 WL 3303861 (E.D. Pa. Dec 2, 2005).
67 *Sony Computer Entertainment Am., Inc. v. Filipiak*, 2005 WL 3556676 (N.D. Cal. Dec. 27, 2005).
68 *DaimlerChrysler Motors v. Bill Davis Racing, Inc.*, 2005 WL 3502172 (E.D. Mich. Dec. 22, 2005).
69 *Samsung Elec. Co., Ltd. v. Rambus, Inc.*, 2006 WL 2038417 (E.D. Va. July 18, 2006).
70 *In re September 11th Liability Ins. Coverage Cases,* 243 F.R.D. 114 (S.D.N.Y. 2007).
71 *S. New England Tel. Co. v. Golbal NAPs, Inc.,* 2008 WL 2704495 (D. Conn. July 1, 2008).