

# Electronic Discovery:

## An Overview Of The Power And The Pitfalls

Bradley C. Nahrstadt

Hanson L. Williams

*Electronic discovery can be expensive, time-consuming and risky, but it's necessary, and it's here to stay.*

---

**COMPUTERS HAVE** changed our everyday lives. They have changed the way we obtain information, the way we shop, and the way we conduct business. They have also changed the way we conduct litigation. Today, when engaging in discovery, it is absolutely essential that requests are made for the production of computerized data. And today, "it is black letter law that computerized data is discoverable if relevant." *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995

U.S. Dist. LEXIS 16335 (S.D. N.Y., Nov. 3, 1995). So it is vitally important for attorneys to understand the nature and extent of electronic data, the means available to preserve that data at the beginning of a lawsuit, who must bear the costs of producing electronic data, how such data should be requested, and the steps that can be taken to protect electronic data from discovery by the other side. Each of these items will be addressed in turn.

---

Bradley C. Nahrstadt and Hanson L. Williams are partners with Williams Montgomery & John Ltd., in Chicago.

**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. Conrad J. Jacoby, *Electronic Discovery Requests*, 43 For the Def. 39 (Dec. 2001). Common types of material include:

- Email messages;
- Word processing files;
- Spread sheets;
- Diaries;
- Cell phone text messages;
- Textbook information (including data from personal digital assistants);
- Internet use histories; and
- Files downloaded from the Internet.

*Id.* Even though a party may have produced material in a tangible form, chances are the electronic version of that material will contain additional information, such as revisions, deleted material, and typist information, including:

- The date the document was created;
- The author of the document;
- Subsequent edit dates of the document;
- Which users had access to revise the document; and
- The number of versions of the document in existence.

All of this information is not visible on the printed version of the document. *Id.*

### Categories Of Electronic Data

Electronic data essentially falls into three general categories: data files, background information, and electronic mail.

#### Data Files

The data files consist of four general types of information that is processed and stored electronically: active data, archival data, back-up

data, and residual data. 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).

#### Active Data

Active data is readily accessible, and comes in many formats, such as word processing documents, spread sheets, databases, email messages, and electronic calendars. Active data files are accessed through programs such as File Manager and Explorer in the Microsoft windows environment. *Id.* at 1828.

#### Archival Data

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 are then used to assist the user in recreating the file should a malfunction occur. However, until the data is needed, it is archived and stored awaiting a request for delivery.

#### Back-up Data

Back-up data provides access to information in the event of a malfunction because the data 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. *Id.* 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. *Id.* at 1828-1829.

### **Residual Data**

Residual data still exists on disc 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 overwrite the space. *Id.* at 1829. Depending on the size and use of the computer system, it may take weeks or even months to overwrite the space containing the “deleted” information. Carey Sirota Meyer and Kari L. Wraspir, *E-Discovery: Preparing Clients For (And Protecting Them Against) Discovery in the Electronic Information Age* 26 Wm. Mitchell L. Rev. 939, 948 (2000). Additionally, sometimes “deleted” files are only partially overwritten, which enables competent computer forensic experts to recover the remaining parts of the document. *Id.* 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. Murphy, *supra*, at 1829.

### **Background Information**

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.

*Id.*

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. *Id.* at 1830.

### **Non-printing Information**

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 time stamps which indicate 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. *Id.*

### **Email**

The last category of electronic evidence is electronic mail. Email is now among the most popular modes of communication in the work place. The characteristics of email, combined with the number of email messages traveling the data wires of businesses and households, makes it an excellent source for evidence in just about any type of case. *Id.* at 1829. What most users do not realize is that email 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 email message. Moreover, if the author’s employer runs periodic backups of their network, email messages are stored on back-up tapes, making the messages as long lasting as the back-up tape itself. Meyer and Wraspir, *supra*, at 949. In addition, because of the reply and forwarding features of most email systems, email 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. Murphy, *supra*, at 1829.

### ***What "Delete" Really Means***

Users of email occasionally believe that since email messages are easily deleted, they can express frank thoughts and opinions in an email 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 emails are confidential, like telephone communications." R. Mark Halligan, *The Brave New World of Electronic Evidence Discovery*, 92 Ill. B.J. 296, 297 (June 2004). 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. *Id.* at 298. 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.*, 1998 WL 614485 (D.D.C. Sept. 14, 1998), 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 emails written by Microsoft employees discussing precisely how Microsoft intended to obtain a monopoly on the Internet browser market. In *Strauss v. Microsoft Corp.*, 1995 WL 326492 (S.D. N.Y. June 1, 1995), the court allowed the plaintiff to introduce into evi-

dence certain email messages created by the defendant's employees which contained inappropriate sexual and gender-related comments. The court admitted the email messages on the grounds that they were directly relevant to the plaintiffs 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.*, 88 F.3d 142 (2d Cir. 1996), 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 email to his colleagues at the defendant corporation detailing the tactical specifications and overall architecture of the plaintiff's system and the defendant's system.

### ***Wireless Text Is Discoverable, Too***

And anyone who thinks that wireless text message will never play an important role in litigation has only to read the most recent headlines. Text messages had a role in a Medford, Oregon case in which a man convicted of killing his wife had sent email and text messages to terrorize her before her death. Jon Sarche, *Wireless Text Messages Showing Up in Court*, Chicago Daily Law Bulletin, p. 2 (June 7, 2004). In Conyers, Georgia, a 17-year-old boy was arrested for investigation of solicitation of sodomy after a 12-year-old girl's parents complained of sexually explicit messages she had received from the boy. *Id.* And in the Kobe Bryant case, the judge requested copies of text messages Bryant's alleged victim sent to a friend and a former boyfriend within hours of the alleged attack. All of these cases reveal just how important it is to conduct comprehensive electronic discovery in any case.

### Finding The Data

Now that counsel is familiar with the types of data generally available, the question becomes how to locate where that data is stored. The first step in the discovery of electronic media is often the use of interrogatories or depositions to develop information on the computer hardware configuration, the operating system, computer language, programming utilized, and the directory structure. Gary T. Walker and John J. Powers, *Electronic Discovery*, 38 For the Def., 22, 23 (Sept. 1996).

### Discovery Of Storage Protocols

In addition to the foregoing, it may be necessary for a party to propound discovery on the opposing side seeking information regarding how the underlying information is obtained and inputted into the opposing party's computer system, back-up and storage procedures, database maintenance, retention and deletion procedures, access, retrieval, and inquiry protocols. *Id.* In addition, it is often wise to propound written discovery seeking a complete listing of all possible sources of electronic discovery, including hard drives, notebook computers, Personal Digital Assistants, zip drives, CDs, diskettes, tapes, smart cards, memory keys, and other removable media. Patricia Nieuwenhuizen, *Email: The Smoking Gun of the Future*, The Nat'l L. J., B9 (Dec. 11, 2000). Also, it may be advantageous for counsel to seek information regarding the existence of personal computers or servers which are no longer in use, as well as the existence and location of back-up tapes or electronic archives. *Id.* Recognizing the importance of this type of information, a number of courts have held that lawyers should be allowed to conduct discovery concerning how another party generates and stores electronic information. *See, Anderson v. Cornejo*, 1999 WL 543196 (N.D. Ill. July 22, 1999); *Dunn v. Midwestern Indemnity*, 88 F.R.D. 191 (S.D. Ohio

1980); *United States v. Russo*, 480 F.2d 1228 (6th Cir. 1973), *cert. denied*, 414 U.S. 1157 (1974).

### Off-site Generation And Storage

Anyone who is engaged in electronic discovery must keep in mind that electronic data may be generated and/or stored on computing equipment that is not necessarily owned by the company which is the target of the lawsuit in question. Electronic material can potentially reside in several distinct locations. Undoubtedly, the most important source of electronic evidence is the computer system or systems maintained by the responding party. However, it is important to keep in mind that it is possible that relevant material may be stored on the home computers of key individuals employed by a corporate party. In some specialized cases, the courts have recognized the nature of the flexibility of the modern workplace and have upheld the right to check specific employees' home computer systems for relevant material. *See, Simon Property Group v. mySimon*, 194 F.R.D. 639 (S.D. Ind. 2000). In addition, many small companies use outside services, such as Earthlink or America Online, to handle their email. In such cases, it may be necessary to request emails directly from the third-party service. Most of the online service providers have published guidelines under which they will accept subpoenas and how they will respond to subpoenas for information regarding customer email accounts. (*See, e.g.*, <http://legal.web.aol.com/aol/aolpol/civilsubpoena.html> setting forth AOL's guidelines for responding to subpoenas and information requests, including a schedule of charges for responding to information requests).

**PRESERVING ELECTRONIC INFORMATION BEFORE DISCOVERY** • Because electronically stored information is subject to deletion at any time, and because such deleted in-

---

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.

---

formation 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. 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). Despite the need for speed in obtaining information regarding electronically stored data, standard discovery procedures are not geared towards 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 this period.

#### **How To Preserve Data For Discovery**

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. *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. *Id.* at 487. 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. Murphy, *supra*, at 1836.

#### **TRO Or Protective Order**

The second option which exists is obtaining 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. *See, United States v. International Business Machines Corp.*, 58 F.R.D. 556 (S.D.N.Y. 1973).

#### **Notice A Duty To Preserve**

The final option is to simply place all opposing parties on notice, as soon as the summons and complaint have been served, of the duty to preserve relevant evidence, including electronic data. The notice should outline the types of data to be preserved, including active and back-up

data files. The notice should further explain where the information might exist, and should include a request for cancellation of documents and data destruction protocols, both in hard copy and electronic form. *Murphy, supra*, at 1835-1836. The notice should also advise opposing counsel that users of their system should refrain from saving files or loading software to existing drives and peripheral devices and to discontinue compression and defragmentation protocols. Moreover, the notice should warn opposing counsel that any failure to preserve such evidence will be dealt with appropriately under the applicable laws of spoliation. *Id.* at 1836; *Robins, supra*, at 502.

#### THE COST OF ELECTRONIC DISCOVERY

- Responding to electronic discovery requests becomes expensive not so much because of the underlying technology, but because of the immense amount of data that must be collected and reviewed. A single back-up tape may hold well over 50,000 email messages; a company's file server may store in excess of 500,000 documents. Multiplying these figures by the number of computers or back-up tapes to be searched demonstrates the gigantic amount of information at issue in some e-discovery requests. *Jacoby, supra*, at 40.

#### Typical Allocation Of Costs

Generally, under most rules of civil procedure, the respondent bears the cost of gathering and reviewing responsive documents, while the requesting party bears the cost of copying such documents. For example, in the case *In re Brand Name Prescription Drugs Antitrust Litigation*, 1995 WL 360526 (N.D. Ill. June 15, 1995), the court granted the plaintiff's motion to compel the defendant to produce more than 30-million pages of emails and to bear the cost incurred as a result of the production. The court ordered that result despite the fact that the cost of pro-

---

Although most courts follow the standard framework of requiring the producing party to bear the costs associated with the production of electronic discovery materials, not all courts have reached that conclusion.

---

duction would range between \$50,000 and \$70,000 and the defendant would have to create a computer retrieval program in order to recover the emails in question. According to the court, although it seemed unfair to force a party to bear the cost of creating a retrieval program to respond to a document request, "if a party chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk." *In re Brand Name Prescription Drugs Antitrust Litigation*, 1995 WL 360526, at \*2. *See also, Bills v. Kennecott Corp.*, 108 F.R.D. 459 (D. Utah 1985) (ordering the defendant to pay for the costs associated with producing detailed employee information stored on the defendant's computer).

#### Time And Labor Cost

Another cost associated with complying with e-discovery requests is the potential disruption to business that may be caused by responding to the discovery requests. At the same time courts have sought to balance the tension between discovery requests and the business disruption they cause, courts have upheld a party's right to collect electronic data that is not available through other means, even if the col-

lection process has a significant impact on the responding party's business. *Id.*

For example, in the trademark infringement case of *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. 1999), Playboy moved to compel discovery of deleted email messages, arguing that the email could show knowing infringement of their "Playmate of the Year" trademark. The motion was granted and Playboy was given permission to obtain a disc image of the defendant's internet server from which she ran her entire web site. Duplicating this information had the side effect of completely shutting down the defendant's Internet-based business for four to eight hours and caused a measurable loss of revenue. Despite the fact that the defendant would suffer substantiated business disruption as a result of complying with the discovery request, the court felt that the disruption was deemed necessary because the deleted email messages could not be obtained in any other way. *Id.*

### *Requesting Party's Burden*

Although most courts follow the standard framework of requiring the producing party to bear the costs associated with the production of electronic discovery materials, not all courts have reached that conclusion. Some courts have ordered the requesting party to bear the costs of reviewing and retrieving computerized information. *See, e.g., Oppenheimer Funds, Inc. v. Sanders*, 437 U.S. 340 (1978) (holding that Federal Rule of Civil Procedure 23(d) empowers a court to direct the requesting party to bear production burdens and costs in a class action). Other courts have recommended that the parties split the costs of copying such documents. *See, e.g., Sattar v. Motorola*, 138 F.3d 1164 (7th Cir. 1998) (approving the trial court's recommendation that if the defendant was unable to provide the computerized information on conventional computer discs or loan the plaintiff the neces-

sary equipment to review the information, the parties each should bear half of the costs of copying).

### **REQUESTING ELECTRONIC MEDIA AND DATA**

• It is crucial, when drafting e-discovery requests, to provide the responding party with fairly specific directions regarding the information requested and to be produced. One method is to request all files and materials that are relevant to the specific issues raised in the requests without limitation on location. This approach places the burden on the responding party to search all media that it believes may contain responsive material. A second method is to request files and materials that are stored on certain specific types of media, such as desktop computers or back-up tapes. The advantage to this approach is that it leaves the responding party no discretion as to the specific media identified in the request. *Jacoby, supra*, at 42.

Many e-discovery requests attempt to combine both approaches. Such requests may begin with instructions that try to list all possible types of data compilations and hardware devices; the actual requests then focus purely on the subject matter at issue. *Id.*

### **Equipment To Search**

Whether or not interrogatories and depositions are used to identify the best sources of data, a few types of equipment should be routinely listed in discovery requests. The vast majority of useful and relevant electronic data is likely to be found on servers, desktop and laptop computers (both actively used and retired or broken), retired or removed hard drives, back-up tapes, and any device or service that is used to read or otherwise process email (including PDAs). "Out of service" equipment in particular is routinely forgotten when data sweeps are conducted; it is well worth specifying such equipment in discovery requests. *Id.* When re-

questing electronic evidence via written discovery requests, it is vitally important that the responding party is informed that the information requested must be produced from all sources, including systems, local area networks, online services, home computers, hard drives, floppy diskettes, magnetic tapes, CD-ROMs, email, system history files and back-up files. Robins, *supra*, at 505.

### *Discovery Checklist*

One commentator has promulgated an e-discovery checklist for litigators to follow when conducting electronic discovery. Among the things he suggests are the following:

- Drafting interrogatories to obtain an overview of the opposing party's computer network and systems;
- In a federal case, preparing a Rule 30(b)(6) notice of deposition for the opposing party's information technology staff;
- Specifying the types of electronic evidence to be produced and the formats for production;
- Questioning every key witness about company policies and his or her habits regarding the use of computers and the storage of company-related electronic data, including storage on home computers and other personal equipment;
- Questioning every key witness about calendars, expense reports, diaries and timesheets and develop a clear record of the hardware and software used for the creation and transmission of such information;
- Questioning every key witness about the habits of other key witnesses relating to the creation, use and storage of electronic data; and
- Questioning every key witness about document retention, email, and Internet policies, as well as those governing use of personal computers for company business.

Halligan, *supra*, at 298.

**HOW TO PROTECT ELECTRONIC DOCUMENTS FROM DISCOVERY** • As with all other discovery, computer or electronic data is discoverable only if the requests propounded by the opposing party satisfies the requirements necessary for the production of the data. Meyer and Wraspir, *supra*, p. 944. In other words, the information must be relevant to the subject matter of the lawsuit; not unnecessarily cumulative or duplicative; the burden or expense must not outweigh its benefit; and it must not be subject to a claim of privilege nor protected by the work product doctrine. *Id.*

### **Relevance**

Given that the relevance threshold is low—"reasonably calculated to lead to the discovery of admissible evidence"—this objection typically will not result in an order prohibiting the production of the information requested. However, in some cases, a relevance objection may be proper when a request asks, for example, for an entire computer hard drive, or similar component, or when the hard drive itself is not part of the subject matter at issue, contains irrelevant information, and the request could be stated in terms of specific categories of information. *See, e.g., In re Grand Jury Subpoena Duces Tecum*, Dated November 15, 1993, 846 F. Supp. 11, (S.D.N.Y. 1994).

### **Undue Burden And Expense**

The most fertile ground for thwarting electronic discovery is the undue burden and expense objection. When faced with a burdensome objection, courts consider whether "the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake...and the importance of the proposed discovery in resolving the issues." Federal Rule of Civil Procedure 26(b)(2)(iii).

Although courts have been quite generous in permitting broad discovery of electronic data, some courts have refused to allow production of electronic data based on speculation or suspicions alone, or where the responding party would be subjected to extremely cumbersome and expensive procedures in producing the information requested. A few illustrative cases include:

- *Alexander v. FBI*, 188 F.R.D. 111 (D.D.C. 1998) (refusing to require defendants to completely restore all deleted files and email when plaintiff did not propose “targeted and appropriately worded searches of backed-up and archived email and deleted hard drives for a limited number of individuals”);
- *Fennell v. First Step Designs, Ltd.*, 83 F.3d 526 (1st Cir. 1996) (affirming district court’s refusal to permit plaintiff access to defendant’s computer system because plaintiff had failed to offer sufficient threshold evidence of the defendant’s supposed alteration or fabrication of evidence);
- *Lawyers Title Ins. Corp. v. United States Fidelity & Guar. Co.*, 122 F.R.D. 567 (N.D. Cal. 1988) (rejecting party’s request to inspect the responding party’s computer system when the requesting party supported its request for such access with only speculation that the responding party might not have produced relevant data);
- *Strasser v. Yalamanchi*, 669 So.2d 1142 (Fla. Dist. Ct. App. 1996) (quashing a district court order granting plaintiff unfettered access to defendant’s computer system where plaintiff had not proven the information was retrievable).

### Attorney-Client And Work Product

Finally, electronic data may be protected from disclosure pursuant to either the attorney-client privilege or the work product doctrine. The attorney-client privilege is applied to protect confidential communications between a client and his or her attorney where the attorney

is acting in his professional legal capacity and the client is seeking legal advice. Courts have refused to compel parties to produce email communications which the court has deemed to be protected by the attorney-client privilege. *See, e.g., IBM Corporation v. Comdisco, Inc.*, 1992 WL 52143 (Del. Super. Ct., March 11, 1992).

The work product privilege is generally used to protect an attorney’s mental impressions, opinions, and legal conclusions prepared in anticipation of litigation. When deciding work product applicability, courts will consider whether the claimed work product is “ordinary work product” or “opinion work product.” *Murphy, supra*, at 1847. Ordinary work product is subject to disclosure if the requesting party makes a showing of substantial need, coupled with an inability to obtain the information from a different source without undue hardship. On the other hand, opinion work product “enjoys a very nearly absolute immunity and can be discovered only in very rare and extraordinary circumstances.” *Id.* Some courts have held that a party can be required to produce electronic evidence which is protected only by the ordinary work product doctrine. *See, e.g., In re Chrysler Motors Corporation Overnight Evaluation Program Litigation*, 860 F.2d 844 (8th Cir. 1988).

**THE ZUBULAKE OPINIONS** • Beginning in 2003, Judge Shira A. Scheindlin, a federal judge in the United States District Court for the Southern District of New York, began issuing a series of opinions regarding electronic discovery. Those opinions, which all revolve around a specific case of alleged employment discrimination, are a must read for any lawyer dealing with the issue of electronic discovery.

Judge Scheindlin’s original opinion, *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) (Zubulake I), sets forth the basic facts of the plaintiff’s cause of action. Laura Zubulake was employed by UBS Warburg as a director

and senior salesperson on its U.S. Asian Equities Sales Desk. She claimed that over the course of a little more than two years, her work product was ridiculed, she was excluded from work-related outings, she was sexually harassed, and subjected to a hostile work environment. When she was eventually terminated by UBS, she filed suite against UBS Warburg and its subsidiaries under federal, state and city laws prohibiting gender discrimination and illegal retaliation.

As part of her discovery requests, Zubulake asked for “all documents concerning any communication by or between UBS employees concerning Plaintiff.” *Zubulake*, 217 F.R.D. at 312. The term “document” was defined to include, “without limitation, electronic or computerized data compilations.” *Id.* In response to the plaintiff’s request, the defendants produced 350 pages of documents, including 100 pages of emails. The plaintiff then asked the defendants to produce all of the emails that had been composed about her that were stored on the company’s back-up tapes. The defendants refused to do so, stating that it would cost approximately \$300,000 to produce the emails that were located on the back-up tapes. The plaintiff then filed a motion to compel.

After initially determining that the defendants’ electronic data was relevant to the plaintiff’s claims, the court spent the majority of the opinion discussing who should bear the cost of producing that data. The plaintiff argued that UBS should have to pay for the costs associated with producing the data stored on the back-up tapes and optical discs. UBS argued that the plaintiff should have to pay the costs associated with production of the data. Faced with these competing arguments, the court recognized that it would have to address the issue of cost shifting (i.e., shifting the cost of production from the party producing the documents to the party requesting the documents).

According to the court, cost-shifting may effectively end discovery, especially when private parties are engaged in litigation with large corporations. As a result, cost-shifting should be considered only when electronic discovery imposes an “undue burden or expense on the responding party.” *Id.* at 318. The burden or expense of discovery is, in turn, “undue” when it “outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.” *Id.*

According to the *Zubulake* court, the key issue in determining whether the production of electronic documents is unduly burdensome or expensive turns primarily on whether the documents are stored in an accessible or inaccessible format. And whether electronic data is accessible or inaccessible turns largely on the media on which it is stored. According to the court, there are essentially five categories of data, listed in order from most accessible to least accessible:

- *Active, online data.* The data that is used in the very active stages of an electronic record’s life—when it is being created or received and processed. One example of online data is the computer’s hard drive;
- *Near-line data.* This typically consists of a robotic storage device that houses removable media and uses multiple read/write devices to store and retrieve records. Examples include optical discs;
- *Off-line storage/archives.* Removable optical disc or magnetic tape media, which can be labeled and stored in a shelf or rack. Off-line storage of electronic records is traditionally used for making disaster copies of records and also for records considered “archival” in that their likelihood of retrieval is minimal;

- *Back-up tapes.* A device, like a tape recorder, that reads data from and writes it onto a tape. Tape drives have data capacities of anywhere from a few hundred kilobytes to several gigabytes. They are generally sequential-access devices, which means that to read any particular block of data, you need to read all the preceding blocks.
- *Erased, fragmented or damaged data.* When a file is first created and saved, it is laid down on the storage media in contiguous clusters. As files are erased, their clusters are made available again as free space. Eventually, some newly created files become larger than the remaining free space and the files are broken up and placed throughout the storage medium. Such fragmented files, along with damaged and erased data, can only be accessed after significant processing.

*Id.* at 318-319. Of the five categories of data, the first three (active, on-line data, near-line data and off-line storage) are typically identified as accessible and the last two (back-up tapes and erased, fragmented or damaged data) are considered inaccessible.

### **Factors In Cost-Shifting**

UBS kept their deleted emails on back-up tapes, a category of data that the court deemed to be inaccessible. Given this fact, the court decided that it was appropriate to consider cost-shifting. The court set forth a seven-factor test to be used in determining when cost-shifting is appropriate. According to Judge Scheindlin, the seven factors to be considered by a court when determining whether to shift the costs include:

- The extent to which the request is specifically tailored to discover relevant information;
- The availability of such information from other sources;
- The total cost of production, compared to the amount in controversy;
- The total cost of production, compared to the resources available to each party;
- The relative ability of each party to control costs and its incentive to do so;
- The importance of the issues at stake in the litigation; and
- The relative benefits to the parties of obtaining the information.

*Id.* at 322.

According to the *Zubulake* court, the first two factors are the most important, the next three factors are moderately important, the sixth factor will rarely come into play and the last factor is the least important since it is fair to presume that the response to a discovery request generally benefits the requesting party. Based on all of the foregoing, the court stated that it believed that requiring UBS to restore and produce responsive documents from a small sample of requested back-up tapes would help the court determine precisely how the costs of production should be assessed. As a result, the court ordered that UBS was to produce, at its expense, responsive emails from any five back-up tapes selected by the plaintiff. UBS was then directed to prepare an affidavit detailing the results of its search, as well as the time and money spent to conduct the search. After reviewing the contents of the tapes and UBS's affidavit, the court indicated that it would conduct the appropriate cost-shifting analysis.

As directed by the court, UBS produced emails from the five back-up tapes selected by the plaintiff. The costs of retrieving and reviewing those five tapes was \$19,003.43. UBS estimated that it would cost \$273,649.39 to retrieve and review emails from the 90 other back-up tapes and again argued that the plaintiff should have to bear the costs associated with retrieving and reviewing the emails contained on those tapes.

The court, after reviewing this information, undertook a cost-shifting analysis. *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003) (*Zubulake III*). It applied the seven-factor test first outlined in *Zubulake I*. The court found that the first two factors tipped slightly against cost-shifting. The court further found that the third and fourth factors weighed against cost-shifting. The fifth and sixth factors were neutral and, according to the court, the seventh factor weighed in favor of cost shifting.

Following this analysis, the court ordered that UBS was to pay for 75 percent of the costs associated with restoring the back-up tapes and the plaintiff was to pay 25 percent of the costs. The court further ordered that UBS, as the responding party, was responsible for paying 100 percent of the costs associated with reviewing and producing the electronic data to the plaintiff.

After the parties began the process of restoring the back-up tapes, they discovered that three back-up tapes were missing and parts of four other tapes could not be located. As a result, the plaintiff asked that the defendant be required to pay in full the costs of restoring the back-up tapes that were located, that an adverse inference instruction be given with respect to the missing back-up tapes and that UBS be ordered to bear the costs associated with re-depositing certain witnesses concerning issues raised in the newly produced emails. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003) (*Zubulake IV*).

The court began its analysis by reiterating that “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 in future litigation.” *Zubulake*, 220 F.R.D. at 216. In this case, the court held that the duty to preserve evidence arose, at the latest, on August 16,

2001, when Zubulake filed her charge with the EEOC.

According to the court, once the duty to preserve evidence attaches, a party (or anticipated party) must retain all relevant documents in existence at the time the duty to preserve attaches as well as any relevant documents created thereafter. In the court’s words, “[o]nce 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.” *Id.* at 218.

Judge Scheindlin said the following about “litigation holds”:

“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 disaster 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.”

*Id.*

The court recognized that three back-up tapes containing the email files of four of the key employees of the defendant (containing emails created prior to the plaintiff’s filing of her EEOC charge) were lost despite a directive to maintain those tapes. The court further recognized that two other lost tapes were made during the time period after the plaintiff filed

her EEOC complaint. UBS offered no explanation for the loss of those tapes.

After determining that the defendant had lost relevant evidence, the court then analyzed the appropriate sanction. The court refused to order that UBS would have to pay for the costs associated with retrieving emails from the remaining back-up discs. The court also refused to give an adverse inference instruction, finding that the plaintiff had not sufficiently demonstrated that the lost tapes contained relevant information. The court did order, however, that UBS was to bear the costs incurred by the plaintiff in re-deposing certain witnesses for the limited purpose of inquiring into issues raised by the destruction of evidence and any newly discovered emails.

During the re-depositions required by *Zubulake IV*, the plaintiff learned about the existence of emails preserved on the defendant's active servers that were never produced to the plaintiff, learned that several UBS employees were systematically destroying emails regarding the plaintiff and learned that several more back-up tapes had been permanently destroyed by the defendant. The plaintiff also uncovered evidence that counsel for the defendant had failed to request retained information from one key employee and failed to give the litigation hold instructions to another. Defense counsel also failed to adequately communicate with another employee how she maintained her computer files. The plaintiff moved for sanctions and again asked that an adverse inference instruction be given to the jury. *Zubulake v. UBS Warburg LLC*, 2004 WL 1620866 (S.D.N.Y. July 20, 2004) (*Zubulake V*).

In ruling on the plaintiff's motion for sanctions, the court said the following about counsel's duty to monitor compliance with a litigation hold:

"Counsel must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce the 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."

*Zubulake*, 2004 WL 1620866, at \*7-8.

### **Complying With The Preservation Obligation**

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 litiga-

tion 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.

Judge Scheindlin concluded, based on all the evidence presented to her, that UBS acted willfully in destroying potentially relevant information, 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 infer-

ence instruction concerning the deleted emails 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.

**CONCLUSION** • 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.

## PRACTICE CHECKLIST FOR

### Electronic Discovery: An Overview Of The Power And The Pitfalls

Electronic discovery can unearth crucial information in a case, but conducting it presents a special set of problems. The best approach is to know what kind of information you might be able to find, approaching electronic discovery as part of the comprehensive discovery plan, and giving some thought to whether cost-shifting might be possible.

- The kinds of information you can find electronically (and where) include:
  - Active, online data. The data that is used in the very active stages of an electronic record’s life—when it is being created or received and processed. One example of online data is the computer’s hard drive;
  - Near-line data. This typically consists of a robotic storage device that houses removable media and uses multiple read/write devices to store and retrieve records. An example includes the optical disc;
  - Off-line storage/archives. Removable optical disc or magnetic tape media, which can be labeled and stored in a shelf or rack. Off-line storage of electronic records is traditionally used for making disaster copies of records and also for records considered “archival” in that their likelihood of retrieval is minimal;

- Back-up tapes. A device, like a tape recorder, that reads data from and writes it onto a tape. Tape drives have data capacities of anywhere from a few hundred kilobytes to several gigabytes. They are generally sequential-access devices, which means that to read any particular block of data, you need to read all the preceding block;
- Erased, fragmented, or damaged data. When a file is first created and saved, it is laid down on the storage media in contiguous clusters. As files are erased, their clusters are made available again as free space. Eventually, some newly created files become larger than the remaining free space and the files are broken up and placed throughout the storage medium. Such fragmented files, along with damaged and erased data, can only be accessed after significant processing.
- Among the things to do as part of your electronic discovery efforts are:
  - Drafting interrogatories to obtain an overview of the opposing party's computer network and systems;
  - In a federal case, preparing a Rule 30(b)(6) notice of deposition for the opposing party's information technology staff;
  - Specifying the types of electronic evidence to be produced and the formats for production;
  - Questioning every key witness about company policies and his or her habits regarding the use of computers and the storage of company-related electronic data, including storage on home computers and other personal equipment;
  - Questioning every key witness about calendars, expense reports, diaries and timesheets and developing a clear record of the hardware and software used for the creation and transmission of such information;
  - Questioning every key witness about the habits of other key witnesses relating to the creation, use and storage of electronic data; and
  - Questioning every key witness about document retention, email, and Internet policies, as well as those governing use of personal computers for company business.
- Although the general rule remains that the responding party must bear the cost of responding some factors in whether costs might be shifted include:
  - The extent to which the request is specifically tailored to discover relevant information;
  - The availability of such information from other sources;
  - The total cost of production, compared to the amount in controversy;
  - The total cost of production, compared to the resources available to each party;
  - The relative ability of each party to control costs and its incentive to do so;
  - The importance of the issues at stake in the litigation; and
  - The relative benefits to the parties of obtaining the information.

To purchase the online version of this article, go to [www.ali-aba.org](http://www.ali-aba.org) and click on "online".