The Sedona Conference Journal

Volume 5 2004

The (2004) *Sedona Principles*: Best Practices, Recommendations & Principles for Addressing Electronic Document Production

The Sedona Conference

Recommended Citation: The Sedona Conference, *The (2004) Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 5 SEDONA CONF. J. 151 (2004).

For this and additional publications see:
https://thesedonaconference.org/publications

THE (2004) SEDONA PRINCIPLES: BEST PRACTICES, RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION

The Sedona Conference Working Group on Electronic Document Retention and Production
Sedona, AZ

Editor's Note: The March 2003 public comment draft of *The Sedona Principles* was included in Vol. 4 of this Journal. This is the 2004 post-public comment version. A brief discussion of the changes follows this reprinting of *The 2004 Sedona Principles*.

I. INTRODUCTION

Discovery in a World of Electronic Documents and Data

Discovery, and document production in particular, is a familiar aspect of litigation practice for many lawyers. The explosive growth and diversification of electronic methods of creating documents, communicating, and managing data has transformed the meaning of the term "document." While 20 years ago PCs were a novelty and e-mail did not exist, today by some estimates more than 90 percent of all information is created in an electronic format.

For courts and lawyers, whose practices are steeped in tradition and precedent, the pace of technological and business change presents a particular challenge.[1] In recent years, courts and litigants have attempted to meet this challenge, sometimes by resorting to traditional approaches to discovery, sometimes by innovating. This paper seeks to synthesize the current and provide new, practical standards for a new form of discovery.

1. What is Electronic Discovery?

Electronic discovery refers to the discovery of electronic documents and data. Electronic documents include e-mail, web pages, word processing files, computer databases, and virtually anything that is stored on a computer. Technically, documents and data are "electronic" if they exist in a medium that can only be read through the use of computers. Such media include cache memory, magnetic disks (such as computer hard drives or floppy disks), optical disks (such as DVDs or CDs), and magnetic tapes. Electronic discovery is often distinguished from "paper discovery," which refers to the discovery of writings on paper that can be read without the aid of some devices.

For readers less familiar with technical terms relevant to electronic discovery, Appendix A contains a glossary of terms.

1 "[I]t has become evident that computers are central to modern life and consequently also to much civil litigation. As one district court put it in 1985, '[c]omputers have become so commonplace that most court battles now involve discovery of some computer-stored information.'" 8A *CHARLES ALAN WRIGHT, ARTHUR R. MILLER, & RICHARD L. MARCUS, FEDERAL PRACTICE & PROCEDURE*, Section 2218 at 449 (2d ed. 1994) (quoting *Bills v. Kennecott Corp.*, 108 F.R.D. 459, 462 (D. Utah 1985)). Similarly, the *Manual for Complex Litigation (Third)* recognizes that the benefits and problems associated with computerized data are substantial in the discovery process. *Manual for Complex Litigation (Third)*, Section 21.446 (Fed. Jud. Ctr. 1995).

2. What Rules Govern Electronic Document Production?

The same rules that govern paper discovery, such as Federal Rules of Civil Procedure 1, 26, and 34, govern electronic discovery. Federal Rule of Civil Procedure 34 permits the service by one party upon another of a request for documents of any type:

> Any party may serve on any other party a request … to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect and copy, any designated documents (including writings, drawings, graphs, charts, photographs, phonorecords, and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form), or to inspect and copy, test, or sample any tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served.

FED. R. CIV. P. 34(a). The Advisory Committee Notes for the 1970 amendments to the rule make clear that the added reference to "data compilations" served to include all forms of electronic data: "The inclusive description of 'documents' is revised to accord with changing technology. It makes clear that Rule 34 applies to electronics [sic] data compilations from which information can be obtained only with the use of detection devices." FED. R. CIV. P. 34, Advisory Committee Notes 1970.

Thus, it is now "black letter law that computerized data is discoverable if relevant." *Anti-Monopoly, Inc. v. Hasbro, Inc.*, No. 94 Civ. 2120, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995); *see also Bills v. Kennecott Corp.*, 108 F.R.D. 459, 463-64 (D. Utah 1985) ("information stored in computers should be as freely discoverable as information not stored in computers"); *Simon Prop. Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 640 (S.D. Ind. 2000) ("[C]omputer records … are documents discoverable under FED. R. CIV. P. 34.").

For all discovery, of course, the Federal Rules protect parties from unduly burdensome, unnecessary, or inefficient discovery. Rule 26 requires that any requested discovery be relevant. Rule 1 provides that that the Federal Rules be "administered to secure the just, speedy, and inexpensive determination of every action." FED. R. CIV. P. 1. The most specific protections against burdensome, unnecessary, or inefficient discovery appear in Rules 26(b) and (c).

Rule 26(b) allows a court to weigh the potential relevance of requested documents against the burden on the party that would have to produce the documents. Rule 26(b)(2)(iii) provides for limiting discovery when "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 in the litigation, and the importance of the proposed discovery in resolving the issues." Rule 26(b)(2)(i) provides that discovery may be limited if "the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive."

Similarly, Rule 26(c) allows a court to enter a protective order against burdensome discovery.

> Upon motion by a party or by the person from whom discovery is sought, accompanied by a certification that the movant has in good faith conferred

> or attempted to confer with other affected parties in an effort to resolve the dispute without court action, and for good cause shown, the court in which the action is pending or alternatively, on matters relating to a deposition, the court in the district where the deposition is to be taken may make any order which justice requires to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense.

FED. R. CIV. P. 26(c).[2]

These broad powers enable a court to limit discovery of electronic documents or condition their production on cost-shifting if the court concludes that the burden of the discovery outweighs its ultimate benefit. The Advisory Committee Notes for the 1970 amendments to the Federal Rules specifically recognized that electronic discovery may generate a special need for such protections against oppressive discovery:

> [W]hen … data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into usable form. In many instances, this means that respondent will have to supply a print-out of computer data. The burden thus placed on respondent will vary from case to case, *and the courts have ample power under Rule 26(c) to protect respondent against undue burden or expense, either by restricting discovery or requiring that the discovering party pay costs.* Similarly, if the discovering party needs to check the electronic source itself, the court may protect respondent with respect to preservation of his records, confidentiality of nondiscoverable matters, and costs.

FED. R. CIV. P. 34, Advisory Committee Notes 1970 (emphasis supplied).

These existing rules, however, do not fully address the distinct nature of electronic documents, and courts must take great care in applying the rules in the electronic context. For example, an inartfully worded order compelling production of electronic records could cause a litigant to incur costs that are multiples of the value of the case before discovery even begins. To fairly apply the Federal Rules to electronic discovery, one must understand the differences between electronic documents and paper documents.

3. How are Electronic Documents Different from Paper Documents?

If the same rules govern paper discovery and electronic discovery, why should electronic discovery be any different from paper discovery? *Byers v. Illinois State Police*, 53 Fed.R.Serv.3d 740, No. 99 C 8105, 2002 WL 1264004 (N.D. Ill. May 31, 2002), which presented a typical electronic discovery dispute, posed this very question:

> The plaintiffs move the Court for an order compelling the defendants to produce archived e-mails that were authored by one of the individual defendants and relate to either plaintiff. The defendants argue that it would be unduly burdensome for them to search the backup tapes containing the archived e-mail. The plaintiffs respond that computer-based discovery is no different than paper-based discovery.

2 Local court rules often contain standards imposing limitations on all forms of discovery.

Id. at *10.

The answer to this question—"why is electronic discovery different?"—lies in the subtle, but sometimes profound, ways in which electronic documents present unique opportunities and problems for document production. In *Byers*, Magistrate Judge Nolan reflected on some of these differences:

> Computer files, including e-mails, are discoverable. However, the Court is not persuaded by the plaintiffs' attempt to equate traditional paper-based discovery with the discovery of e-mail files. Chief among these differences is the sheer volume of electronic information. E-mails have replaced other forms of communication besides just paper-based communication. Many informal messages that were previously relayed by telephone or at the water cooler are now sent via e-mail. Additionally, computers have the ability to capture several copies (or drafts) of the same e-mail, thus multiplying the volume of documents. All of these e-mails must be scanned for both relevance and privilege. Also, unlike most paper-based discovery, archived e-mails typically lack a coherent filing system. Moreover, dated archival systems commonly store information on magnetic tapes which have become obsolete. Thus, parties incur additional costs in translating the data from the tapes into useable form."

Id. at *31-33. There are many ways in which producing electronic documents is qualitatively and quantitatively different from producing paper documents. They can be grouped into six broad categories of differences.

A. Volume and Duplicability

First and foremost, there are vastly more electronic documents than paper documents, and electronic documents are created at much greater rates than paper documents. As a result, the amount of information available for potential discovery has exponentially increased with the introduction of electronic data. For example, the use of e-mail has risen dramatically in recent years. In 1998, the U.S. Postal Service processed approximately 1.98 billion pieces of mail. During that year, there were approximately 47 million e-mail users in the United States who sent an estimated 500 million e-mail messages per day, for a total of approximately 182.5 billion e-mail messages per year—more than 90 times as many messages as the U.S. Postal Service handled the same year. In 2003, it is projected that there will be 105 million e-mail users in the United States, who will send over 1.5 billion e-mail messages a day (approximately 547.5 billion e-mail messages per year)—nearly as many messages in a day as the U.S. Postal Service handles in a year.

The dramatic increase in e-mail usage and electronic file generation poses special problems for large corporations. A single large corporation can generate and receive millions of e-mails and electronic files each day. At least 93 percent of information created today is first generated in digital format,[3] 70 percent of corporate records may be stored in electronic format,[4] and 30 percent of electronic information is never printed to paper.[5] Not surprisingly, the proliferation of the use of electronic data in corporations has resulted in vast accumulations. While a few thousand paper documents are enough to fill a file cabinet, a single computer tape or disk drive the size of a small book can hold the equivalent of

3 Kenneth J. Withers, *The Real Cost of Virtual Discovery*, 7 FEDERAL DISCOVERY NEWS 3 (Feb. 2001).
4 Lori Enos, *Digital Data Changing Legal Landscape*, E-Commerce Times, May 16, 2000.
5 Richard L. Marcus, *Confronting the Future: Coping with Discovery of Electronic Material*, 64 Law & Contemp. Probs. 253, 280-81 (Spring/Summer 2001).

millions of printed pages. Organizations often accumulate thousands of such tapes as data is stored, transmitted, copied, replicated, backed up, and archived.

Partly responsible for this phenomenon is the fact that electronic documents are more easily duplicated than paper documents. Electronic information is subject to rapid and large scale user-created and automated replication without degradation of the data. E-mail provides a good example. E-mail users frequently send the same e-mail to many recipients. These recipients, in turn, often forward the message, and so on. At the same time, e-mail software and the systems that are used to transmit the messages automatically create multiple copies as the messages are sent and resent. Similarly, other business applications are designed to periodically and automatically make copies of data. Examples of these include web pages that are automatically saved as cache files and file data that is routinely backed up to protect against inadvertent deletion or system failure.[6]

B. Persistence

Second, electronic documents are more difficult to dispose of than paper documents. A shredded paper document is essentially irretrievable.[7] Likewise, a paper document that has been discarded and taken off the premises is generally considered to be beyond recovery. Disposal of electronic documents is another matter altogether. "The term 'deleted' is sticky in the context of electronic data. 'Deleting' a file does not actually erase the data from the computer's storage devices. Rather, it simply finds the data's entry in the disk directory and changes it to a 'not used' status—thus permitting the computer to write over the 'deleted' data. Until the computer writes over the 'deleted' data, however, it may be recovered by searching the disk itself rather than the disk's directory. Accordingly, many files are recoverable long after they have been deleted—even if neither the computer user nor the computer itself is aware of their existence." *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 313 n.19 (S.D.N.Y. 2003) ("*Zubulake I*") (internal quotation marks omitted). This persistence of electronic data compounds the rate at which electronic data and documents accumulate and creates an entire subset of electronic data that exists unknown to the individuals with ostensible custody over them. Indeed, because of the difficulty of effectively deleting electronic documents, software is sold that purports to completely erase or "wipe" the data by overwriting the data numerous times.

C. Dynamic, Changeable Content

Third, computer information, unlike paper, has dynamic content that is designed to change over time even without human intervention. Examples include: workflow systems that automatically update files and transfer data from one location to another; tape backup applications that move data from one cartridge to another to function properly; web pages that are constantly updated with information fed from other applications; and e-mail systems that reorganize and remove data automatically. As a result, unlike paper documents, many electronic documents and collections are never fixed in a final form.

More generally, electronic documents are more changeable than paper documents. Documents in electronic form can be modified in numerous ways that are sometimes difficult to detect without computer forensic techniques. Moreover, the act of merely

6 Neither the users who created the data nor information technology personnel are necessarily aware of the existence and locations of the replicant copies. For instance, a word processing file may reside concurrently on an individual's hard drive, in a network-shared folder, as an attachment to an e-mail, on a backup tape, in an Internet cache, and on portable media such as a CD or floppy disk. Furthermore, the location of particular electronic files typically is determined not by their substantive content, but by the software with which they were created, making organized retention and review of those documents difficult.

7 Modern technology, however, has made recovery at least a theoretical possibility. *See* Douglas Heingartner, *Back Together Again*, New York Times, July 17, 2003, at G1 (describing new technology that can reconstruct cross-shredded paper documents).

accessing or moving electronic data can change it. For example, booting up a computer can alter data contained on it. Simply moving a word processing file from one location to another can change creation or modification dates. In addition, drafts of documents may be retained without the user's knowledge or consent.

D. Metadata

Fourth, electronic documents, unlike paper, contain information that is known as "metadata." Metadata is information about the document or file that is recorded by the computer to assist the computer and often the user in storing and retrieving the document or file at a later date. The information may also be useful for system administration as it reflects data regarding the generation, handling, transfer, and storage of the data within the computer system. Much metadata is not normally accessible by the computer user.

There are many examples of metadata. Such information includes file designation, create and edit dates, authorship, comments, and edit history. Indeed, electronic files may contain hundreds or even thousands of pieces of such information. For instance, e-mail has its own metadata elements that may include, such information as the dates that mail was sent, received, replied to or forwarded, blind carbon copy ("bcc") information, and sender address book information.

Indeed, an e-mail message may routinely have over a thousand different metadata elements. Typical word processing documents have hidden codes that determine whether to indent a paragraph, change a font, and set line spacing. The ability to recall inadvertently deleted information is another familiar function, as is tracking of creation and modification dates. Similarly, electronically created spreadsheets may contain calculations that are not visible in a printed version or completely hidden columns that can only be viewed by accessing the spreadsheet in its native application. Internet documents contain hidden data that allow for the transmission of information between an Internet user's computer and the server on which the internet document is located. So-called "meta-tags" allow search engines to locate websites responsive to specified search criteria. "Cookies" are embedded codes that can be placed on a computer (without user knowledge) that can, among other things, track usage and transmit information back to the originator of the cookie.[8]

Metadata presents unique issues for the preservation and production of documents in litigation. On the one hand, it is easy to conceive of situations where metadata is necessary to authenticate a document, or establish facts material to a dispute, such as when a file was accessed in a suit involving theft of trade secrets. In most cases, however, the metadata will have no material evidentiary value—it does not matter when a document was printed, or who typed the revisions, or what edits were made before the document was circulated. And there is also the real danger that information recorded by the computer may be inaccurate. For example, when a new employee uses a word processing program to create a memorandum by using a memorandum template created by a former employee, the metadata for the new memorandum may incorrectly identify the former employee as the author.

Understanding when metadata needs to be specifically preserved and produced represents one of the biggest challenges in electronic document production.

E. Environment-Dependence and Obsolescence

8 An extensive discussion of the problems raised by metadata can be found in Jason R. Baron's article *Recordkeeping in the 21st Century*, 33 Information Management Journal 8 (July 1999) (available at http://www.arma.org/pdf/journal/1999/7_99_02.pdf).

Fifth, electronic data, unlike paper data, may be incomprehensible when separated from its environment.[9] For example, as a structured set of data, the information in a database may be incomprehensible when removed from the structure in which it was created. If the raw data (without the underlying structure) in a database is produced, it will appear as merely a long list of undefined numbers. To make sense of the data, a viewer needs the context that includes labels, columns, report formats, and other information. Existing or customized "reports" based on queries of the database can be generated without producing the entire database.

Also, the frequent obsolescence of computer systems due to changing technology creates unique issues for recovering electronic documents that are not present in the recovery of paper documents. It is not unusual for an organization to undergo several migrations of data to different platforms within a few years. Moreover, because of the turnover in computer systems, neither the personnel familiar with the obsolete systems nor the technological infrastructure necessary to restore the out-of-date systems may be available when this "legacy" data needs to be accessed. In a perfect world, electronic records that have continuing value for business purposes or litigation are converted for use in successor systems, and all other data is discarded. In reality, though, such migrations are rarely flawless.

F. Dispersion and Searchability

Sixth, while an employee's paper documents will often be consolidated in a handful of boxes or filing cabinets, the employee's electronic documents could reside in numerous locations: desktop hard drives, laptop computers, network servers, floppy disks, and backup tapes. Many of these electronic documents may be identical backup copies. However, some documents may be earlier versions drafted by that employee or by other employees who can access those documents through a shared network.

Consequently, it may be more difficult to determine the provenance of electronic documents than paper documents. The ease of transmitting electronic data and the routine modification and multi-user editing process may obscure the origin of a document. Electronic files are often stored in shared network folders that may have departmental or functional designations rather than author information. In addition, there is growing use of collaborative software that allows for group editing of electronic data, rendering the determination of authorship far more difficult. Finally, while electronic documents may be stored on a single drive, it is likely that such documents may also be found on high-capacity, undifferentiated backup tapes, or on network servers—not under the custodianship of an individual who may have "created" the document.

Counterbalancing, to some extent, the dispersed nature of electronic documents is the fact that some forms of electronic documents and some forms of electronic media can be searched quickly and fairly accurately by automated methods. For these types of electronic documents, software may be able to search through far more documents than human beings could hope to review manually.

4. Why Do Courts and Litigants Need Standards Tailored to Electronic Discovery?

The differences between electronic documents and paper documents make clear that document production will mean very different things in the electronic and the paper

9 In addition, passwords, encryption, and other security features can limit the ability of users to access electronic documents.

contexts. In practical terms, these differences mean that rules principally designed to govern paper documents do not always provide meaningful guidance for disputes involving the discovery of electronic documents.

For example, a preservation order to save "all records pertaining to the manufacture of X" could, if all documents were paper documents, be applied logically by a party, which could instruct employees to collect and preserve those records. In the electronic age, such a command could present intractable problems. Because electronic information is both dynamic and ubiquitous, a party would have to, unless it suspended operations, copy all electronic data, wherever located and in whatever form, for possible production. That process could be extraordinarily complex and expensive, depending upon the size of the data involved, since it is typically impossible to suspend destruction of only the information covered by the preservation order.[10]

The Working Group has first-hand experience of unreasonable and unfair burdens in producing electronic documents in litigation. These unfair burdens have included, among other things, spending millions of dollars to process and review large volumes of electronic documents that had little likelihood of being relevant to the case and preserving at great cost thousands of backup tapes that were subsequently not even sought by the opposing party later in discovery.

We believe that the unfair burdens would be minimized if standards were provided to parties and courts for addressing electronic document production. Without standards, parties are left to guess as to what their obligations are, with the threat of discovery violations for incorrect guesses. Indeed, a number of courts facing electronic discovery issues have noted the lack of principled guidance in the area. For example, the court in *McPeek v. Ashcroft* observed, in the context of evaluating the discovery of e-mail backup tapes:

> [t]here is certainly no controlling authority for the proposition that restoring all backup tapes is necessary in every case. The Federal Rules do not require such a search, and the handful of cases are idiosyncratic and provide little guidance. The one judicial rationale that has emerged is that producing backup tapes is a cost of doing business in the computer age. *In re Brand Name Prescription Drugs,* Nos. 94 C 897, MDL 997, 1995 WL 360526 at *3 (N.D. Ill., June 15, 1995). But, that assumes an alternative. It is impossible to walk ten feet into the office of a private business or government agency without seeing a network computer, which is on a server, which, in turn, is being backed up on tape (or some other media) on a daily, weekly or monthly basis. What alternative is there? Quill pens?

McPeek v. Ashcroft, 202 F.R.D. 31, 33 (D.D.C. 2001) (footnote omitted). The general lack of standards has been noted by other judges as well. *See, e.g.*, Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. Rev. 327, 361 (2000) ("[W]hile courts have managed to resolve motions that raise Rule 34 questions in the context of electronic discovery, they have generally approached these questions in a highly fact-specific manner, producing few general principles to aid in the resolution of similar disputes.").[11]

10 Indeed, at an extreme, such data might be interpreted to include machine or product line data that is collected only for milliseconds. Attempting to retain all such data would effectively shut down manufacturing operations because its retention would quickly outstrip the storage capacity.

11 There are many examples of conflicting guidance in the case law. *Compare, e.g., McPeek v. Ashcroft*, 202 F.R.D. at 33 (restoring all backup tapes not necessary in every case) *with Linnen v. A.H. Robins Co.*, 10 Mass. L. Rptr 189, No. 97-2307, 1999 WL 462015, at *9-10 (Mass. Super. June 16, 1999) (obligation imposed to cease recycling of backup tapes); *compare, e.g., In re Brand Name Prescription Drugs Antitrust Litig.*, Nos. 94 C 897, MDL 997, 1995 WL 360526, at *2 (N.D. Ill. June 15, 1995) (holding that producing party must bear costs, as would be the case with paper documents, because the producing party chose to store the data electronically), *with Rowe Entm't, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 421 (S.D.N.Y. Jan. 16, 2002) (adopting multiple factor test to address cost allocation of electronic discovery burden).

5. How Can Courts and Litigants Use Precedent from the Context of Paper Discovery in the Context of Electronic Documents?

Recognizing the differences between electronic and paper document production begs the crucial question: what to do with the great body of case law applying the Federal Rules in the context of paper discovery? How can courts and counsel use familiar applications of the Rules to guide discovery in the unique context of electronic documents?

To answer this question, one should consider the two obvious alternative approaches: a "similarity" paradigm that seeks guiding principles in precedent by searching for analogies to electronic discovery in the paper context and following the guidelines that would apply in the paper context; and a "difference" paradigm that emphasizes the differences between electronic and paper documents and rejects the guidance of paper discovery cases because of these differences. Both approaches offer useful insights, but neither approach will ultimately serve the interests of litigants or the courts.

A. Sameness: Find an Analogy from Paper Discovery

There is a temptation in the face of new legal terrain to search for analogies to familiar cases that could provide guidance. Often such an exercise can be illuminating, and indeed many principles from paper discovery appear to be sound in the context of electronic document production.

> *Illustration i.* Searches for relevant paper documents usually entail identifying the files of key individuals or files devoted to the individual, product, or conduct that is at issue in the litigation (such as the personnel file of a plaintiff who is suing for unlawful termination). There is no expectation that an organization search the filing cabinets of employees with no connection to the issues in the litigation. Thus, by analogy, there should be no expectation that an organization search the computer files of individuals with no connection to the litigation.

> *Illustration ii.* The preservation obligation for paper documents does not require a party to keep multiple identical copies of each potentially relevant paper document. Thus, it makes no sense to require a party to preserve electronic documents on optical disks or hard drives as well as the copies of those same documents that might exist on backup tapes.

Drawing analogies from paper discovery, however, can lead to costly pitfalls. These pitfalls arise when parties fail to recognize the distinct capabilities or limitations of electronic documents.

> *Illustration iii*. When reviewing paper documents before production, attorneys and paralegals commonly review each page of a potentially relevant paper file to see if the document mentions a person or event responsive to a document request. It has been common practice with respect to electronic documents to print out paper copies of all potentially responsive documents and then review them by hand. By doing so, however, the responding party foregoes the possibility of greatly reducing the time and cost of document review by using automated searches.

Illustration iv. In the world of paper discovery, a document preservation order requiring that a corporate party "freeze" all of its documents is burdensome, but normally would not force the party to shut down its business. Paper documents can be left in their files, or copied if they need to be marked up. Personnel can suspend their practice of throwing away old files. But in the electronic context, complying with such an order and freezing all electronic information (including shared or interactive databases) could be catastrophic to a business.

It may be literally impossible to "freeze" a company's electronic documents without shutting down its entire computer system, because data are altered and overwritten constantly on all computer systems, often in ways that users cannot detect or control. For example, the mere act of accessing a document can alter it, and on any given system, thousands of temporary files are created and overwritten daily, hourly, or more frequently. Disk space that is no longer in use, but which may contain potentially relevant fragmented data, may also be overwritten.

B. Difference: Eschew Precedent from Paper Discovery

Appreciating the differences between electronic and paper documents can allow courts and parties to break from past practice in ways that serve the goals of the Federal Rules: "just, speedy, and inexpensive" resolution of litigation. For example, as noted above, automated searches may be faster and less expensive than a page-by-page manual review of electronic documents. And as noted by the *Byers* court, a 20-year-old box of papers and a 20-year-old backup tape are not comparable subjects of discovery. The paper documents may be yellowed, but still readable, while the electronic documents on the backup tape may be written in code that can only be read by software that no longer exists. *See Byers*, 2002 WL 1264004, at *10. Yet it may not be advisable to do things differently simply because new technology makes it possible.

Illustration v. It may be easier to recover "destroyed" electronic documents than "destroyed" paper documents. Computer forensic techniques allow parties to recover or reconstruct deleted documents even, in some cases, documents that appear to have been permanently deleted. But this does not mean that parties responding to document requests should be required to produce deleted data or data fragments. The expense and disruption caused by such techniques would not justify such a production. Here, an analogy to paper is useful. Must a producing party produce papers that it threw away a year ago? Or must it reassemble and copy shredded documents in the garbage cans? *See Rowe Entm't, Inc. v. The William Morris Agency, Inc.*, 205 F.R.D. 421, 431 (S.D.N.Y. 2002) ("Just as a party would not be required to sort through its trash to resurrect discarded paper documents, so it should not be obligated to pay the cost of retrieving deleted e-mails."). Of course, whether in the paper or electronic context, if there is a serious question of document destruction, recovering destroyed documents may be justified. Even paper documents that have been shredded to confetti possibly can be reconstructed using new, sophisticated (but expensive) technology. *See* Douglas Heingartner, *Back Together Again*, New York Times, July 17, 2003, at G1 (describing technology that may be used to reconstruct documents shredded by the East German secret police).

Illustration vi. Because the cost of electronic document storage (*i.e.*, optical disks or magnetic tape) is relatively low, some have suggested preserving copies of electronic documents even when there is no business reason or legal obligation to do so. Yet this overlooks the fact that indiscriminate copying and retention of electronic files—even if cheaper than indiscriminate copying and retention of paper files—leads to the same or greater headaches in litigation: ballooning costs of review for responsiveness and privilege, large numbers of duplicate documents, and problems dealing with retrieving documents in obsolete formats that have been unnecessarily retained.

C. Translation: Applying Media-Neutral Rules in a Context-Specific Way

The best approach to electronic discovery begins by recognizing how existing precedent and new technology interact. The rules governing discovery are, as noted above, broadly stated standards that require reasonableness in their application. As such, the rules governing discovery are *media neutral*, in that they apply to documents existing in all media—paper, electronic, or stone tablets. Due to their generality, however, the proper application of the rules only takes shape when one understands the specific context in which the rule is applied. For electronic discovery, this requires that the litigants and the courts understand how electronic documents work, and the costs and benefits of different approaches to discovery.

The result is a process of *translation*: precedent from the world of paper discovery provides a starting point, composed of the legal rule and the application in the specific facts of the case. One can translate that precedent to the world of electronic discovery by asking whether the factual differences between the paper context and the electronic context are relevant to the rule. If so, the precedent may not be a good model. If not, the paper-based precedent could be an adequate starting point for discovery in the electronic context.

For example, in illustration *i*. above, the controlling, media-neutral rule is that production is limited to relevant documents, and the specific application in the paper context is that employees not connected to the issues in the litigation need not search their files because in all likelihood they will not have any relevant documents. In translating from paper discovery to electronic discovery, the question is, "Does the existence of documents in electronic form make the files of such employees more relevant?" Since the answer is no, the guideline in the paper context translates well to the electronic context.

On the other hand, in illustration *iii*. above, the controlling, media-neutral rule is the obligation to produce documents responsive to a document request. The specific application in this illustration involves the most efficient way to identify responsive documents. In the paper context, paralegals and attorneys commonly conduct a page-by-page review of documents, looking for certain key words. In translating this best practice from paper discovery to electronic discovery, the question is, "Does the existence of documents in electronic form make another technique more efficient?" In this case the answer may be yes, if the electronic documents are in a searchable format. Importantly, correctly answering this question ("translating") requires an understanding of the electronic documents at issue.

The Working Group has examined the issue of electronic document production closely, focusing both on its similarities to and differences from paper document production. The principles that follow reflect our efforts at translating the rules of discovery into the law of electronic document production.

II. THE SEDONA PRINCIPLES FOR ELECTRONIC DOCUMENT PRODUCTION

1. Electronic data and documents are potentially discoverable under FED. R. CIV. P. 34 or its state law equivalents. Organizations must properly preserve electronic data and documents that can reasonably be anticipated to be relevant to litigation.

2. When balancing the cost, burden, and need for electronic data and documents, courts and parties should apply the balancing standard embodied in FED. R. CIV. P. 26(b)(2) and its state law equivalents, which require considering the technological feasibility and realistic costs of preserving, retrieving, producing, and reviewing electronic data, as well as the nature of the litigation and the amount in controversy.

3. Parties should confer early in discovery regarding the preservation and production of electronic data and documents when these matters are at issue in the litigation, and seek to agree on the scope of each party's rights and responsibilities.

4. Discovery requests should make as clear as possible what electronic documents and data are being asked for, while responses and objections to discovery should disclose the scope and limits of what is being produced.

5. The obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.

6. Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronic data and documents.

7. The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronic data and documents were inadequate.

8. The primary source of electronic data and documents for production should be active data and information purposely stored in a manner that anticipates future business use and permits efficient searching and retrieval. Resort to disaster recovery backup tapes and other sources of data and documents requires the requesting party to demonstrate need and relevance that outweigh the cost, burden, and disruption of retrieving and processing the data from such sources.

9. Absent a showing of special need and relevance a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual data or documents.

10. A responding party should follow reasonable procedures to protect privileges and objections to production of electronic data and documents.

11. A responding party may satisfy its good faith obligation to preserve and produce potentially responsive electronic data and documents by using electronic tools and processes, such as data sampling, searching, or the use of selection criteria, to identify data most likely to contain responsive information.

12. Unless it is material to resolving the dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court.

13. Absent a specific objection, agreement of the parties or order of the court, the reasonable costs of retrieving and reviewing electronic information for production should be borne by the responding party, unless the information sought is not reasonably available to the responding party in the ordinary course of business. If the data or formatting of the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information should be shifted to the requesting party.

14. Sanctions, including spoliation findings, should only be considered by the court if, upon a showing of a clear duty to preserve, the court finds that there was an intentional or reckless failure to preserve and produce relevant electronic data and that there is a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.

III. PRINCIPLES & COMMENTS

1. Electronic data and documents are potentially discoverable under FED. R. CIV. P. 34 or its state law equivalents. Organizations must properly preserve electronic data and documents that can reasonably be anticipated to be relevant to litigation.

Comment 1.a. The Importance of Proper Document Management Policies

Organizations should adopt policies that provide rational and defensible guidelines on the treatment of electronic documents. These guidelines should be created after considering the business, regulatory, and tax needs of the organization, including the need to conserve electronic storage space on e-mail and other servers. Thus, a company that determines it only needs to retain e-mail with business record significance could set forth these guidelines in its document retention policy. Employees would then be responsible for implementing the policy and neither destroying documents prematurely nor retaining documents beyond their useful life. Any such system should include provisions for litigation holds to preserve documents related to ongoing or reasonably anticipated litigation, governmental investigations, or audits. The existence and reasonable effectiveness of such a program should be a significant consideration in any spoliation analysis.[12]

The advantages of an effective document retention program are particularly pronounced with respect to distributed data and disaster recovery backup tapes. An effective document retention program, combined with a preservation approach triggered by the reasonable anticipation of litigation, would establish the principal source of discovery material, thus reducing the need to routinely access and review multiple sources of likely duplicative data, including backup tapes. An appropriate electronic document preservation program would involve most or all of the following:

- Establishing a thorough but practical records management program and training individuals to manage and retain business records created or received in the ordinary course of business;

12 Of course, no organization can ensure 100% percent compliance with its records management program, but this limitation inheres in all document retention, whether paper or electronic.

- Helping business units establish practices and customs, tailored to the needs of their businesses, to identify the business records they need to retain;

- Implementing a system of presumptive limits (based on time or quantity) on the retention of e-mail and other communications, such as instant messaging and voice-mail, to the extent their content does not merit treatment as business records, and developing communications policies that promote the appropriate use of company systems;

- Determining the recycle time applicable to backup tapes based on disaster recovery needs;

- Developing and implementing appropriate procedures to identify and notify relevant individuals and business units of the need to preserve electronic and other records for reasonably anticipated or pending litigation; and

- Establishing and maintaining awareness of the importance of preserving potential evidence in the case of threatened litigation, and training lawyers and business people on when and how to carry out their responsibilities.

Implementing policies with features such as those described above can provide a solid basis to plan for the treatment of electronic documents during discovery. By following an objective, preexisting policy, an organization can formulate its responses to electronic discovery not by expediency, but by reasoned consideration.[13] Under such an approach, a responding party may be able to limit its discovery responses to producing only those materials that are reasonably available to it in the ordinary course of business.

Comment 1.b. The Benefits of Written Records Management Policies

A written records management policy can enable an organization to ensure that it is retaining all records necessary to the business, regulatory, and legal needs of the organization. Indeed, the Code of Federal Regulations "has over 1500 references to reporting and record keeping requirements." J. Edwin Dietel, *Designing an Effective Records Retention Compliance Program* Section 1:26 (2002). While not all of these regulations will apply to any one organization, any organization that does business in the United States will be subject to at least some of these regulations.

A written records management policy can also provide guidance on how to properly dispose of documents—both written and electronic—that are without use to the organization. Under such programs, an organization can demonstrate that it has legitimately destroyed documents by following reasonable and objective standards. Indeed, at least one court has held that the existence of a reasonable records management policy, instituted and applied in good faith, should be considered in determining whether to apply sanctions based on the destruction of evidence. *See Lewy v. Remington Arms Co.*, 836 F.2d 1104, 1112 (8th Cir. 1988) ("[I]f the trial court is called upon to again instruct the jury regarding the failure to produce evidence, … [f]irst, the courts should determine whether Remington's record management policy is reasonable considering the facts and circumstances surrounding the relevant document. … Second, in making this determination the court may also consider

13 Doing so will help protect against a possible spoliation claim. For example, in *Lewy v. Remington Arms Co.*, 836 F.2d 1104, 1112 (8th Cir. 1988), the United States Court of Appeals for the Eighth Circuit held that, before giving a jury instruction regarding failure to produce evidence, a court should consider whether the party alleged to have destroyed evidence had a records retention policy that was "reasonable considering the facts and circumstances surrounding the relevant documents[,] … whether lawsuits concerning the complaint or related complaints have been filed, the frequency of such complaints, [ ] the magnitude of the complaints[, and] whether the retention policy was instituted in bad faith."

whether lawsuits concerning the complaint or related complaints have been filed, the frequency of such complaints, and the magnitude of the complaints. Finally, the court should determine whether the document retention policy was instituted in bad faith."); *see also Willard v. Caterpillar, Inc.*, 40 Cal. App. 4th 892, 921 (Cal. 1995) (The "good faith disposal pursuant to a bona fide consistent and reasonable document retention policy could justify a failure to produce documents in discovery."). If an organization implements a clearly defined written records management policy that establishes parameters for what records need to be kept, then destruction of records not meeting these retention guidelines is defensible. However, an organization cannot employ a records management policy designed to obstruct discovery. *See Stevenson v. Union Pac. R.R. Co.*, ___ F.3d ___ 2003 WL 23104550, at *8 (8th Cir. Jan. 5, 2004) (after receipt of specific request for documents, company "cannot rely on its routine document retention policy as a shield" for destruction of evidence); *Kozlowski v. Sears, Roebuck & Co.*, 73 F.R.D. 73 (D. Mass. 1976) (cannot use policies to thwart discovery obligations).

Comment 1.c. Written Records Management Policies Should Account for Records in Both Paper and Electronic Form

An organization can benefit from creating a records management policy designed to ensure that all information needed to conduct the business of the organization, fulfill its legal and financial recordkeeping requirements, and preserve its institutional memory is maintained and accessible while providing for the appropriate disposition of other documents. Because a modern organization's records are created and exist in both paper and electronic form, an organization's records management policy should address both paper and electronic documents. Such policies can enable organizations to maximize the value of their accumulated information, including electronically stored information, and appropriately view records as assets in which the organization has invested substantial capital. *See generally Pub. Citizen v. Carlin,* 2 F. Supp.2d 1 (D.D.C. 1997) (noting that "computers have now become a significant part of the way the federal government conducts its business" and therefore "[t]he federal government must adapt its electronic recordkeeping capabilities to reflect that reality."), *rev'd on other grounds*, 184 F.3d 900 (D.C. Cir. 1999), *cert. denied*, 529 U.S. 1003 (2000).

In some instances, an organization can address electronic and paper records with a single set of policies that require identical treatment of paper and electronic materials. In other instances, however, appropriate treatment of both paper and electronic materials will require records management policies that differentiate between paper and electronic materials.

Comment 1.d. Preservation in the Context of Litigation

An organization's document retention policies should focus on the business needs of the organization and the budgetary constraints on its use of technology. An organization also must retain documents that may be relevant to current or reasonably anticipated litigation. *See* Principle 5 and associated commentary. Further, most organizations are subject to statutory and regulatory regimes that require the preservation of particular documents for specified periods of time. For example, the Sarbanes-Oxley Act of 2002, 116 Stat. 745 (2002), contains a number of document preservation requirements applicable to many publicly traded companies.

Beyond satisfying these legal duties, however, it is neither feasible nor reasonable for organizations to take extraordinary measures to preserve documents if there is no business or regulatory need to retain such documents and there is no reasonable anticipation

of litigation to which those documents may be relevant. For example, some commentators have observed that organizations should consider routinely making mirror image copies of employee disk drives when an employee leaves an organization or when computer equipment is recycled or discarded. While there may be unusual circumstances when that is advisable, as a general rule it would be wasteful and wholly unnecessary to accumulate such massive quantities of unused data just because it is technically possible to do so. Rather, in accordance with existing records management principles, it is more rational to establish a procedure by which selected items of value can be identified and retained as necessary to meet the organization's legal and business needs during changes in personnel or hardware.

2. When balancing the cost, burden, and need for electronic data and documents, courts and parties should apply the balancing standard embodied in FED. R. CIV. P. 26(b)(2) and its state law equivalents, which requires considering the technological feasibility and realistic costs of preserving, retrieving, producing, and reviewing electronic data, as well as the nature of the litigation and the amount in controversy.

Comment 2.a. Scope of Reasonable Inquiries

The traditional approach to preserving and producing paper documents has been to identify and inform appropriate individuals of the specific need to preserve reasonably available information that may be relevant to the dispute at issue. This is followed by reasonable steps to gather and produce documents, after review for privilege, trade secrets, or other appropriate bases for non-production.

A similar approach is also proper to identify, preserve, and produce relevant information in electronic format. The Federal Rules did not intend to place a new, different, and greater discovery obligation upon litigants with relevant electronic information merely because of the increased volume of potential materials involved. Instead, litigants should start with these traditional foundations for good faith compliance with discovery obligations and employ the unique capabilities of computer tools to assist in identifying, locating, retrieving, preserving, reviewing, and producing relevant electronic data and documents.

Comment 2.b. Balancing Need and Cost of Electronic Discovery

The standard of Rule 26(b), requiring a balancing of the need for discovery with the burdens imposed, is particularly applicable to discovery of electronic documents and data. Among the factors that must be addressed in electronic discovery are: (a) large volumes of data, (b) data being stored in multiple repositories, (c) complex internal structures of collections of data and the relationships of one document to another, (d) data in different formats and coding schemes that may need to be converted into text to be understood by humans, and (e) frequent changes in information technology. In this context, the need to accurately balance Rule 26(b) factors becomes particularly acute.

Electronic discovery burdens must be proportional to the amount in controversy and nature of the case. Otherwise, transaction costs due to electronic discovery will overwhelm the ability to resolve disputes fairly in litigation. *See, e.g., Alexander v. FBI,* 188 F.R.D. 111, 117 (D.D.C. 1998) (limiting discovery to "targeted and appropriately worded searches of backed-up and archived e-mail and deleted hard-drives for a limited number of individuals"); *Zonaras v. General Motors Corp.*, No. C-3-94-161, 1996 WL 1671236, at *4 (S.D. Ohio Oct. 17, 1996) (relying on proportionality test of Federal Rules to determine that benefits of discovery outweigh expense).

Costs cannot be calculated solely in terms of the expense of computer technicians to retrieve the data, but must factor in other litigation costs. For instance, the court in *In re General Instrument Corporation Securities Litigation* noted that, while retrieval of the requested documents from backup tapes was not unduly expensive, the implications of a production order requiring that act were broader:

> [T]he technical matter of retrieving the documents from the backup tapes would be just the start of the process. Defense counsel would then have to read each e-mail, assess whether the e-mail was responsive, and then determine whether the e-mail contained privileged information. Given that the volume of e-mail at issue here is potentially very large, the court finds that the burden of reviewing the requested documents would be heavy.

In re Gen. Instr. Corp. Sec. Litig., No. 96 C 1129, 1999 WL 1072507, at *6 (N.D. Ill. Nov. 18, 1999). In addition, the non-monetary costs (such as the invasion of privacy of business data, and the risks to business and legal confidences and privileges) and secondary economic costs (including the burdens on information technology personnel and the resources required to review documents) should be considered in any calculus of whether to allow discovery.

Comment 2.c. Need to Coordinate Internal Efforts

Decisions regarding preserving electronic documents and data are typically a team effort, involving counsel (inside and outside), information systems professionals, end-user representatives, records management personnel, and, potentially, other individuals with knowledge of the relevant computer systems and how data is used, such as information security personnel. Parties may use outside consultants, and include them in some of the team activities when consistent with the need for privileged communications.

The team approach permits each team member's relevant expertise to be applied regarding preservation issues. Furthermore, maintaining a team allows the organization to build a knowledge base about its systems and how they are used. The organization may identify a person or persons who will act as the organization's spokesperson or witness on issues relating to the scope of electronic document production. Of course, the size and responsibilities of any team will likely vary greatly depending upon the size of the organization and the scope of litigation. Coordination of information and effort is essential. *See Keir v. UnumProvident Corp.*, No. 02 Civ. 8781, 2003 WL 21997747, at *5-9 (S.D.N.Y. Aug. 22, 2003) (vague directions and lack of coordination led to loss of data subject to preservation order).

Comment 2.d. Communications with the Court Regarding Electronic Data Collection and the Need to Develop an Adequate Factual Record

Organizations should take reasonable positions when arguing electronic data collection issues in court. The organization must clearly demonstrate that it will fulfill its responsibility to preserve and produce relevant data. Overstated or excessive cost estimates will reduce the organization's credibility. Where feasible, the organization should promptly implement a fair and reasonable plan for collecting and producing data, rather than leaving the court to rule on competing plans. When an organization does not present the court with a reasonable plan, the court will usually err on the side of protecting the integrity of the data collection process and require preservation exceeding what may be reasonably necessary.

In preparing for court conferences, counsel needs to adequately consult with their clients' information technology departments and vendors regarding the technical issues involved in data preservation. *See Keir v. UnumProvident Corp.*, No. 02 Civ. 8781, 2003 WL 21997747, at *12 (S.D.N.Y. Aug. 22, 2003) (specifically noting counsel's failure to inform court of burdens and technological issues regarding preservation order); *see also Landmark Legal Foundation v. EPA*, 272 F. Supp.2d 70, 77-79 (D.D.C. 2003) (reciting failures of agency's attorneys to properly communicate preservation order to agency and holding that agency committed contempt of court by reformatting hard drives and erasing e-mail backup tapes after it received notice of the order). When providing affidavits or testimony to the court on these issues, the organization should recognize that judges may lack technical background. Resources should be directed to develop presentations that make complex technical issues comprehensible to the court.

3. Parties should confer early in discovery regarding the preservation and production of electronic data and documents when these matters are at issue in the litigation and seek to agree on the scope of each party's rights and responsibilities.

Comment 3.a. Parties Should Include Electronic Discovery Issues in Their Rule 26 Disclosures and Conferences

Federal Rule of Civil Procedure 26(f) requires parties to confer early in litigation to attempt to develop a discovery plan. *See In re Bristol-Myers Squibb Sec. Litig.*, 205 F.R.D. 437, 441 (D.N.J. 2002) (where party possesses relevant information in electronic format, it is obligated to advise adversary under mandatory disclosure rules); *Kleiner v. Burns,* No. 00-2160, 2000 WL 1909470, at *4 (D. Kan. Dec. 15, 2000) (holding that Rule 26 requires disclosure of nature and location of relevant electronic documents).

The Rule 26(f) conference is an important tool that can avoid disputes over discovery of electronic documents. In fact, several United States District Courts have, via local rule, mandated that such conferences explicitly include discussion of electronic discovery issues. *See* U.S. Dist. Ct. Ark. L. R. 26.1 ("The FED. R. CIV. P. 26(f) report filed with the court must contain the parties' views and proposals regarding … [w]hether any party will likely be requested to disclose or produce information from electronic or computer-based media. If so [the report must also specify details on the anticipated electronic discovery]."); U.S. Dist. Ct. N.J. L. R. 26.1(d) ("During the FED. R. CIV. P. 26(f) conference, the parties shall confer and attempt to agree on computer-based and other digital discovery matters."); U.S. Dist. Ct. Wyo. L. R. 26.1(d)(3)(B) ("The parties shall meet and confer regarding the following matters during the FED. R. CIV. P. 26(f) conference: (i) Computer-based information (in general) … (ii) E-mail information … (iii) Deleted information … and (iv) Back-up data.").

By early discussion of issues such as which computer systems will be subject to preservation and discovery, the relevant time period, and the identities of particular individuals likely to have relevant electronic documents, litigants can identify and attempt to resolve disputes before they create collateral litigation. *See, e.g., In re Bristol-Myers Squibb Sec. Litig.*, 205 F.R.D. at 444 ("counsel should take advantage of the required Rule 26(f) meeting to discuss issues associated with electronic discovery").

Creating checklists of key issues to consider during an electronic discovery conference can guide the parties and minimize the likelihood of post-discovery spoliation

disputes.[14] Counsel should also be prepared to discuss electronic discovery issues during the Rule 16(b) pretrial conference with the court, whether required by local rule or not.

> *Illustration i.* A party seeking production of e-mails requests that all backup tapes, hard drives, laptops, PDAs, and other computer systems in the organization be preserved. The request makes no provision for ongoing operation of computer systems and does not narrow the request to reasonable persons, subjects and types of devices covered. After informal consultations, the parties are able to agree upon resolution of the issues (such as which databases contain records that will be preserved) and their agreement is embodied in a letter.
>
> *Illustration ii.* Plaintiffs in a lawsuit involving allegations of securities fraud against multiple defendants seeking extensive damages request preservation of electronic documents by all defendants. The defendants, most of whom are large investment banks and other financial institutions, respond that preservation obligations need to be tailored so that they are defined, manageable, and cost-effective while also preserving evidence that is truly needed for the resolution of the dispute. The parties meet and confer upon a protocol for preserving existing data, including preserving select (not all) backup tapes, certain archived data, select legacy systems, distributing retention notices (and updates), creating a limited number of mirror images of select computer hard drives, undertaking measures to collect potentially relevant data, and distributing a questionnaire regarding electronic data systems. The defendants assess the costs and burdens involved in the various proposed steps and reach agreement on the scope and limitations of the obligations. The protocol averts motion practice and provides certainty as to the expected preservation efforts. *Cf.* Case Management Order Relating to Preservation of Electronic Data, *In Re Initial Public Offering Sec. Litig.*, 21 MC 92 (SAS) (S.D.N.Y. Dec. 19, 2002) (adopting parties' proposed Protocol for the Preservation of Electronic Data).

Comment 3.b. Privilege Logs for Voluminous Electronic Documents

> Federal Rule of Civil Procedure 26(b)(5) states that:
>
> [w]hen a party withholds information otherwise discoverable under these rules by claiming that it is privileged or subject to protection as trial preparation material, the party shall make the claim expressly and shall describe the nature of the documents, communications, or things not produced or disclosed in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the applicability of the privilege or protection.

Traditionally, parties have complied with this rule by producing a privilege log with separate entries for each document that contains objective information about the document (such as author, addressee and Bates number) as well as a field that describes the basis for the privilege claim. Even if there are few documents, preparing a privilege log is often extremely

14 *See, e.g.*, Kenneth J. Withers, Computer-Based Discovery in Federal Civil Litigation, 2000 Fed. Cts. L. Rev. 2, at Appendix A (http://www.fclr.org/2000fedctslrev2.htm). In addition, the November 17, 2003 draft amendments to the *ABA Civil Discovery Standards* have proposed another checklist of issues for consideration. *See* Nov. 17, 2003 ABA draft at Standard 13 ("Effective Use of Discovery Conferences").

time consuming. Even with the best efforts of counsel it often results in a privilege log that is of marginal utility at best. *See Mitchell v. Nat'l R.R. Passenger Corp.*, 208 F.R.D. 455, 461 (D.D.C. 2002) ("While FED. R. CIV. P. 26(b)(5) requires what lawyers call a 'privilege log,' I have held that such logs are nearly always useless. Instead, defendants will now be required to submit all documents as to which a privilege is claimed, to chambers for an *in camera* review."); *see also Avery Dennison Corp. v. Four Pillars,* 190 F.R.D. 1, 2 (D.D.C. 1999) (noting that "counsel rarely provides more than minimal information in the logs they submit"). The immense volume of electronic documents now being poured into the litigation process exacerbates this unavoidable problem.

One solution that parties should consider at the outset is to agree to accept privilege logs that will initially classify categories or groups of withheld documents, while providing that any ultimate adjudication of privilege claims if challenged will be made on the basis of a document-by-document review. The basis for this approach is the 1993 rules amendment comment to Rule 26(b)(5), which states:

> The rule does not attempt to define for each case what information must be provided when a party asserts a claim of privilege or work product protection. Details concerning time, persons, general subject matter, etc., may be appropriate if only a few items are withheld, but may be unduly burdensome when voluminous documents are claimed to be privileged or protected, particularly if the items can be described by categories.

FED. R. CIV. P. 26, Advisory Committee Notes 1993. An agreement at the outset of litigation to log privileged documents by category that provides for a fair and full defense of individual privilege claims if challenged, will reduce motion practice regarding log deficiencies and other procedural challenges that are becoming more common given the huge volume of documents at issue.

Comment 3.c. Preservation of Expert Witness Drafts and Materials

The obligation to preserve and produce electronic data may apply to expert witness testimony. The 1993 amendments to Rule 26(a)(2)(B) require the disclosure of all "information considered by the [expert] in forming the [expert's] opinion." Under this standard, courts have held that the failure to preserve data and information could lead to sanctions and exclusion of testimony. *See, e.g., Trigon Ins. Co. v. United States,* 204 F.R.D. 277, 282-84, 289-91 (E.D. Va. 2001) (finding that government had duty to preserve correspondence between experts and consultants, including drafts of expert reports; that the destruction of such evidence was intentional, warranting sanctions for spoliation of evidence; and that an adverse inference against the experts' testimony and their credibility in general was warranted). It is not hard to imagine that litigants will quickly adapt the electronic spoliation disputes of document discovery to the realm of expert witness disclosures (for example, requests for all of the electronic copies of expert witness reports, for access to the expert's hard drive to search for deleted data, or requests for access to all e-mail accounts of the expert).

Because of this potential for dispute, and recognizing that the issue will almost always affect both parties, the best course for the parties is to discuss, early in the case, the issue of which expert witness materials need to be preserved and exchanged in accordance with Rule 26(a)(2)(B). If an agreement cannot be reached, it is far preferable to approach the court with a sensible solution early in a disputed motion than to face accusations of evidence spoliation later.

4. Discovery requests should make as clear as possible what electronic documents and data are being asked for, while responses and objections to discovery should disclose the scope and limits of what is being produced.

Comment 4.a. Requests for Production Should Clearly Specify What Documents are Being Requested

A requesting party that believes in good faith that particular electronic documents should be reviewed by the producing party in responding to document requests should request those documents clearly and with particularity.

Such discovery requests should go beyond boilerplate definitions seeking all e-mail, databases, word processing files, or whatever other electronic documents the requesting party can generally describe. Instead, the request should target particular electronic data that the requesting party contends is important to resolve the case. By identifying relevant documents, parties can avoid the sort of blanket, burdensome requests for electronic documents that invite blanket objections and judicial intervention.

The requesting party should also identify the form in which it wishes the data to be produced. *See* TEX. R. CIV. P. 196.4 ("To obtain discovery of data or information that exists in electronic or magnetic form, the requesting party must specifically request production of electronic or magnetic data and specify the form in which the requesting party wants it produced.").

Comment 4.b. Rule 34 Responses and Objections

Rule 34 responses and objections should indicate that reasonable steps have been taken to produce responsive electronic data and documents. If production has not been made from all reasonably available sources of electronic documents and data, a respondent should tender appropriate objections based upon existing production efforts, cost, burden, overbreadth of the request, and/or other factors.

It is neither reasonable, feasible, nor required under Rule 34 to produce every file or message that might potentially be relevant to every issue in the litigation. It should be reasonable, for example, to limit searches for messages to the e-mail accounts of key witnesses in the litigation, for the same reasons that it has been regarded as reasonable to limit searches for paper documents to the paper files of key individuals. Likewise, it should be appropriate, absent unusual circumstances, to limit review for production to those sources most likely to contain unique, relevant data and information (such as active files or removable media used by key employees). The better practice is to specify such limitations in the responses so that any disputes can be addressed and resolved early.

Comment 4.c. Disclosure of Collection Parameters

It is usually not feasible, and may not even be possible, for most business litigants to collect and review all data from their computer systems in connection with discovery. The extraordinary effort that would be required to do so could cripple many businesses. Yet, without appropriate guidelines, if any data is omitted from a production, an organization may be accused of withholding data that should have been produced. Unnecessary controversy over peripheral discovery issues can often be avoided at the outset by discussion by the parties of the potential scope and related costs of collecting relevant data.

5. The obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.

Comment 5.a. Scope of Preservation Obligation

The common law duty to preserve evidence clearly extends to electronic documents. Indeed, the vast majority of information upon which businesses operate today is generated electronically, and much of this information is never printed to paper. Therefore, organizations must take reasonable steps to preserve electronic documents for litigation, whether pending or reasonably anticipated.

The preservation obligation necessarily involves two related questions: (1) when does the duty to preserve attach, and (2) what evidence must be preserved. *Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243, 2003 WL 22410619, at *2 (S.D.N.Y. Oct. 22, 2003) ("*Zubulake IV*"). The first inquiry remains unchanged in the world of electronic data and documents, although the need to recognize when a duty arises may be more important in light of the volatility of certain data.

The second inquiry is a much greater challenge regarding electronic data and documents. The obligation to preserve relevant evidence is generally understood to require that the producing party make reasonable efforts to identify and manage the relevant information readily available to it. Satisfying this obligation must be balanced against the right of a party to continue to manage its electronic information in the best interest of the enterprise, even though some electronic information is necessarily overwritten on a routine basis by various computer systems. If such overwriting is incidental to the operation of the systems—as opposed to a deliberate attempt to destroy evidence in anticipation of or in connection with an investigation or litigation—it should be permitted to continue after the commencement of litigation. *See* Martin H. Redish, *Electronic Discovery and the Litigation Matrix*, 51 Duke L.J. 561, 621 (2001) ("(1) Electronic evidence destruction, if done routinely in the ordinary course of business, does not automatically give rise to an inference of knowledge of specific documents' destruction, much less intent to destroy those documents for litigation-related reasons, and (2) to prohibit such routine destruction could impose substantial costs and disruptive burdens on commercial enterprises."); *see also Concord Boat Corp. v. Brunswick Corp.*, No. LR-C-95-781, 1997 WL 33352759, at *4 (E.D. Ark. Aug. 29, 1997) ("[T]o hold that a corporation is under a duty to preserve all e-mail potentially relevant to any future litigation would be tantamount to holding that the corporation must preserve all e-mail."). *But see 7 MOORE'S FEDERAL PRACTICE* Section 37A.12[5][e] (Matthew Bender 3d ed.) ("The routine recycling of magnetic tapes that may contain relevant evidence should be immediately halted on commencement of litigation.").

At a minimum, organizations need not preserve every shred of paper, every e-mail or electronic document, and every backup tape. *See Zubulake IV* at *3. To declare otherwise would "cripple large corporations" who are almost always involved in litigation. Id. A reasonable balance must be struck between (1) an organization's duty to preserve relevant data, and (2) an organization's need, in good faith, to continue operations.

> *Illustration i*. L Corporation ("L Corp.") routinely backs up its e-mail system every day and recycles the backup tapes after two weeks. Discovery is served relating to a product liability claim brought against L Corp. arising out of the design of products sold one year ago. L Corp. promptly

and appropriately notifies all employees involved in the design, manufacture, and sale of the product to save all documents, including e-mails relating to the issues in the litigation, and the legal department takes reasonable steps to ensure that all relevant evidence has, in fact, been preserved. L Corp. continues its policy of recycling backup tapes while the litigation is pending. Absent awareness of a reasonable likelihood that specific unique and relevant information is contained only on a backup tape, there is no violation of preservation obligations, because the corporation has an appropriate policy in place and the backup tapes are reasonably considered to be redundant of the data saved by other means.

Comment 5.b. Organizations Must Prepare for Electronic Discovery to Reduce Cost and Risk

The main purpose of an organization's computer system is to assist the organization in its business activities. Nonetheless, the need to respond to discovery in litigation is a fact of life for many organizations.

The costs of responding to requests for discovery of information contained in computer systems can be best controlled if the organization takes steps ahead of time to prepare computer systems, and users of these systems, for the potential demands of litigation.

Such steps include instituting defined, orderly procedures for preserving and producing potentially relevant documents and data, and establishing processes to identify, locate, retrieve, preserve, review, and produce data that may be responsive to discovery requests or required for initial mandatory disclosures. Preparing for electronic discovery can also help the corporation accurately present the cost and burden of specific discovery requests to the court, control the costs of reasonable steps to produce data, and avoid the risk of failing to preserve or produce evidence from computer systems.

Illustration i. Med Corporation ("Med") is a manufacturer of pharmaceutical products. Med has established a three-week rotation for system backups. One of Med's products, LIT, is observed to cause serious adverse reactions in a number of patients, and the FDA orders it withdrawn from the market. Anticipating the potential for claims relating to LIT, Med's litigation department collects all potentially relevant information from employees. The litigation response system helps Med identify and quickly move to preserve all potentially relevant data, including e-mail, user files, corporate databases, shared network areas, public folders, and other repositories. The process results in relevant data being collected on a special litigation database server that is independent of normal system operations and backups.

Eight months later, a class action is filed against Med for LIT injuries. Plaintiff's counsel obtains an *ex parte* order requiring Med to save all of its backup tapes, to refrain from using any auto-deletion functions on e-mail and other data, pending discovery, or to reformat or reassign hard drives from employees involved in any way with LIT. Med's Information Systems department estimates that the order would cost at least $150,000 per month to comply with, including the cost of new tapes, reconfiguration of backup procedures and tape storage, purchase and installation of additional hard drive space for accumulating e-mail and file

> data, and special processing of hard drives when computers are upgraded or employees leave the company or are transferred.
>
> Med promptly moves for relief from the order, demonstrating through its documented data collection process that the relevant data has been preserved, and that the requested modifications of its systems are unnecessary due to the preservation efforts already in place. The court withdraws its order and Med is able to defend the litigation without impact on normal operations of its computer systems or excessive electronic discovery costs.

Comment 5.c. Corporate Response Regarding Litigation Preservation

Ordinarily, organizations should identify and define preservation obligations at the outset of litigation. Due to the dynamic nature of electronic data, delay in taking preservation steps may increase the danger of claims that evidence was not preserved. Early preservation steps can also prevent unnecessary disputes over retention issues.

The duty to comply with a preservation obligation is an affirmative duty. The scope of what is necessary will, of course, vary widely between and even within organizations depending upon the nature of the claims and information at issue. *See Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243, 2003 WL 22410619, at *3 (S.D.N.Y. Oct. 22, 2003) ("In recognition of the fact that there are many ways to manage electronic data, litigants are free to choose how this task [of retaining relevant documents] is accomplished."). That said, organizations addressing preservation issues should carefully consider the future discovery demands for relevant data to avoid needless repetitive steps to capture data again in the future. *See In re Amsted Industries, Inc. "Erisa" Litig.*, 2002 WL 31844956, at *2 (N.D. Ill. Dec. 18, 2002) (requiring defendants to "research their tapes under the broader subject matter and time period" ordered by the court).

Ideally, an effective means of retaining documents reasonably subject to the preservation obligation should be established as soon as practicable. An appropriate notice should be effectively communicated to an appropriate list of affected persons. (*See* Cmt. 5.d, *infra*.) Senior management or legal advisors may need to be involved in the retention decisions and processes, depending upon the particular circumstances. *Cf. In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 F.R.D. 598, 615 (D.N.J. 1997) (court noted that "obligation to preserve documents that are potentially discoverable materials is an affirmative one that rests squarely on the shoulders of senior corporate officers" and found that particular nature of litigation and repeated failure of efforts to preserve documents warranted sanctions); *see also Danis v. USN Communications, Inc.*, No. 98 C 7482, 2000 WL 1694325, at *38-41 (N.D. Ill. Oct. 20, 2002) (circumstances of case indicated insufficient involvement of management in proper oversight and delegation of preservation responsibilities).

Comment 5.d. Notice to Affected Persons

Upon determining that litigation or an investigation is threatened or pending and has triggered a preservation obligation, the organization should take reasonable steps to communicate to affected persons the need for and scope of preserving relevant records (both electronic and hard copy). The form, content and distribution of the notice will vary widely between and among organizations depending upon the circumstances, and there is no talisman.

The notice need not be a detailed catalog of information types to be retained. Instead, it should sufficiently describe the kinds of information that must be preserved so the affected custodians of data can segregate and preserve identified files and data. *See Wiginton v. CB Richard Ellis, Inc.*, No. 02 C 6832, 2003 WL 22439865, at *5 (N.D. Ill. Oct. 27, 2003) (defendant was faulted for being too narrow when preservation communication to employees only instructed employees to save documents that "pertain to" the named plaintiff in a putative class action although various other employees and offices were identified in the complaint).

The notice should state that electronic as well as paper documents must be preserved. The notice might need to specifically address preservation of data in multiple locations (*e.g.*, network, workstation, laptop or other devices), depending upon the circumstances of the organization and the dispute. The notice need not demand preservation of all documents—only those affected by the preservation obligation.

Additionally, the preservation obligation, except in extreme circumstances, should not require the complete suspension of normal document management policies, including the routine destruction and deletion of records. The notice does not need to reach all employees, only those reasonably likely to maintain documents relevant to the litigation or investigation. In many cases, the notice should be sent to a person or persons responsible for the maintaining and operating computer systems or files that have no particular custodian or owner but may fall within the scope of the preservation obligation. *See id.* at *2 (among other problems with preservation notice sent to employees was the defendant's failure "to inform its director of network services that any electronic information should be retained").

Communications should be accomplished in a manner reasonably designed to provide prominent notice to the recipients. Depending upon the scope and duration of the litigation, it may be advisable to repeat the notice periodically in at least one form or location. When preservation obligations apply to documents and data spanning a significant or continuing time period, organizations should analyze whether special steps are needed to deal with hardware that might be retired if it contains unique relevant documents.

> *Illustration i.* Pursuant to its procedures for litigation response, upon receipt of notice of the claim, the organization reasonably identifies the departments and employees involved in the dispute. Those individuals whose files are reasonably likely to contain relevant documents and information are notified via e-mail of the dispute and are asked to take steps to retain documents (including electronic communications, data and records) that may be relevant to the litigation, which is described in the notice. The notice identifies a contact person who can address questions regarding preservation duties. The notice is also distributed to the identified Information Technology liaison, who works with management and legal counsel to identify any systems files or data that may be subject to the preservation obligation.

Parties also should consider whether notice must be sent to third parties, such as contractors and vendors who provide information technology services. This concern arises out of FED. R. CIV. P. 34, which frames a party's obligation in terms of the possession, custody or control of documents. The responding party should set forth any objections to producing a document in the possession of third parties so that any disputes can be resolved early in the litigation.

Comment 5.e. Preservation Obligation Not Ordinarily Heroic

Preservation orders should not impose heroic or unduly burdensome requirements on organizations with electronic documents.[15] A party may request, and a court can compel, the exercise of extraordinary efforts to preserve or produce electronic material that is not readily available in the ordinary course of business. However, this power to order extraordinary efforts should be exercised only where there is a substantial likelihood that the information exists in the form sought, that it would not remain in existence absent intervention, and that its preservation or production is likely to materially advance the interests of justice in the individual case. *See* FED. R. CIV. P. 26(b)(2) ("The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that … 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 in the litigation, and the importance of the proposed discovery in resolving the issues.").

> *Illustration i.* A requesting party seeks an order, over objection, that backup tapes created during a relevant period should be preserved and restored. It develops sufficient proof to raise the likelihood that substantial amounts of deleted but relevant information existed in the time frame covered by the backup tapes. Before ruling on the merits of the request, the court should consider having the producing party restore and search a sample of the tapes to determine the likelihood that relevant and discoverable material, not otherwise available, can be recovered and that it is worthwhile to do so. If recovery of information from the backup tapes is ordered, the court should consider whether further use of sampling techniques would minimize the burdens on the producing party.

Comment 5.f. Preservation Orders

In general, courts should not issue a preservation order unless the party requesting such an order demonstrates at a hearing the necessity of such an order. Because all litigants are obligated to preserve relevant documents in their possession, custody, or control, a party seeking a preservation order must first demonstrate a real danger of document destruction, the lack of any other available remedy, and that a preservation order is an appropriate exercise of the court's discretion. *See Adobe Sys., Inc. v. Sun South Prods., Inc.*, 187 F.R.D. 636, 642-43 (S.D. Cal. 1999) (denying motion for temporary restraining order to permit immediate examination of defendant's computers because of the technical difficulties of permanently destroying electronic documents); *Gorgen Co. v. Brecht,* No. C2-01-1715, 2002 WL 977467, at *2-3 (Minn. Ct. App. May 14, 2002) (overturning temporary restraining order barring defendants from destroying or altering paper or electronic documents because plaintiff failed to demonstrate risk of irreparable harm).

Preservation orders may in certain circumstances aid the discovery process by defining the specific contours of the parties' preservation obligations. In those circumstances, before a preservation order is issued, the parties should attempt to work out the scope and parameters of the preservation obligation through the meet and confer process. Preservation orders should be tailored to require preservation of documents and data that are potentially

15 The 1999 ABA Civil Discovery Standards echo this conclusion, although the November 17, 2003 proposed amendments to this Standard omit this guidance entirely. *Compare ABA Civil Discovery Standards*, Standard 29(a)(iii) (1999) ("[A] party does not ordinarily have a duty to take steps to try to restore electronic information that has been deleted or discarded in the regular course of business ….") *with* Nov. 17, 2003 proposed draft amendments to *ABA Civil Discovery Standards.*

relevant to the case, and should not unduly interfere with the normal functioning of the affected computer systems.

Ex parte preservation orders should be discouraged. Such orders violate the principle that responding parties are responsible for preserving and producing their own electronic documents and data. *See* Principle 6, *infra*. More generally, preservation orders should be issued rarely, and only in cases in which the standards for injunctive relief have been met. *See In re Potash Antitrust Litig.*, No. 3-93-197, MDL No. 981, 1994 WL 1108312, at *7-8 (D. Minn. Dec. 5, 1994) (applying standard for injunctive relief to request for a preservation order); *Humble Oil & Refining Co. v. Harang*, 262 F. Supp. 39, 42-43 (E.D. La. 1966) (same). This is particularly important when dealing with electronic data that may be transitory and not susceptible to reasonable preservation measures. *See Dodge, Warren & Peters Ins. Servs., Inc. v. Riley*, 105 Cal. App. 4th 1414, 1418, 130 Cal. Rptr. 2d 385 (2003) (applying standards for injunctive relief to request to "freeze" defendants' electronically stored data.)

Usually, neither the party seeking a preservation order nor the court will have a thorough understanding of the other parties' computer system, the electronic data that is available, or the mechanisms in place to preserve that electronic data. For example, courts sometimes believe that backup tapes are inexpensive and that preservation of tapes is not burdensome. However, backup systems vary a great deal in this regard, and without information regarding the specifics of the backup system in use, it is difficult to tell what steps may be appropriate or inappropriate for data preservation purposes.

Comment 5.g. All Data Does Not Need to be "Frozen"

A party's preservation obligation does not require freezing of all electronic documents and data, including e-mail. *See Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243, 2003 WL 22410619, at *2 (S.D.N.Y. Oct. 22, 2003) (organizations need not preserve "every shred of paper, every e-mail or electronic document, and every back-up tape."); *see also Wiginton v. CB Richard Ellis, Inc.*, No. 02 C 6832, 2003 WL 22439865, at *4 ("A party does not have to go to extraordinary measures" to preserve all potential evidence … [i]t does not have to preserve every single scrap of paper in its business.") (citing *China Ocean Shipping (Group) Co. v. Simone Metals Inc.*, No. 97 C 2694, 1999 WL 966443, at *3 (N.D. Ill. Sept. 30, 1999) and *Danis v. USN Communications, Inc.*, No. 98 C 7482, 2000 WL 1694325, at *32 (N.D. Ill. Oct. 20, 2000)).

Civil litigation should not create the aura of a crime scene with forensic investigation employed at every opportunity. Theoretically, a party could preserve the contents of waste baskets and trash bins for evidence of statements or conduct. Yet, the burdens and costs of those acts are apparent and no one would typically argue that this is required. There should be a similar application of reasonableness to preservation of electronic documents and data.

Even though it may be technically possible to capture vast amounts of data during preservation efforts, this usually can be done only at massive cost. Data is maintained in a wide variety of formats, locations and structures. Many copies of the same data may exist in active storage, backup, or archives. Computer systems manage data dynamically, meaning that the data is constantly being cached, rewritten, moved and copied. For example, a word processing program will usually save a backup copy of an open document into a temporary file every few minutes, overwriting the previous backup copy. In this context, imposing an absolute requirement to preserve all information would require shutting down computer

systems and making copies of data on each fixed disk drive, as well as other media that are normally used by the system. Costs of litigation would routinely approach or exceed the amount in controversy in most lawsuits. In the ordinary course, therefore, the preservation obligation should be limited to those steps reasonably necessary to secure evidence for the fair and just resolution of the matter in dispute.

> *Illustration i.* In a Freedom of Information Act ("FOIA") action, the district court enters a preliminary injunction that the agency believes requires it to freeze all computers that could potentially contain documents subject to the FOIA dispute. In implementing the order, the agency determines that the categorical freeze on all agency hard drives requires the purchase of new equipment with each personnel change and wherever there are certain types of equipment malfunctions. The agency should approach the court for implementation of a more limited order so that only those computers that contain responsive records will be preserved and all others can be released for reuse. *See* July 10, 2002 Notice of Supplemental Instructions Regarding Preservation of Electronic Information, *Landmark Legal Foundation v. EPA,* No. 00-2338 (RCL) (D.D.C. July 10, 2002).

Comment 5.h. Disaster Recovery Backup Tapes

Absent specific circumstances, preservation obligations should not extend to disaster recovery backup tapes created in the ordinary course of business. *See McPeek v. Ashcroft*, 202 F.R.D. 31, 33 (D.D.C. 2001) ("There is certainly no controlling authority for the proposition that restoring all backup tapes is necessary in every case. The Federal Rules do not require such a search, and the handful of cases are idiosyncratic and provide little guidance.").

When backup tapes exist to restore electronic files that are lost due to system failures or through disasters such as fires or tornadoes, their contents are, by definition, duplicative of the contents of active computer systems at a specific point in time. Thus, employing proper preservation procedures with respect to the active system should render preservation of backup tapes on a going-forward basis redundant. Further, because backup tapes generally are not retained for substantial periods, but are instead periodically overwritten when new backups are made, preserving backup tapes would require the time-consuming and costly process of reprogramming backup systems, manually exchanging backup tapes, and purchasing new tapes or hardware.

In some organizations, however, the concepts of backup and archive are not clearly separated, and backup tapes are retained for a relatively long period of time to provide for retention of files that may need to be accessed in the future. Backup tapes may also be retained for long periods of time out of concern for compliance with record retention laws. Under these circumstances, there is a possibility that the stored backup tapes contain the only remaining copy of data or documents that may be relevant in a case.

Organizations that use backup tapes for archival purposes should be aware that this practice is likely to cause substantially higher costs for evidence preservation and production in connection with litigation. *Compare Rowe Entm't, Inc. v. The William Morris Agency, Inc.*, 205 F.R.D. 421, 429-30 (S.D.N.Y. 2002) (in determining whether to shift costs, considering "the purposes for which the responding party maintains the requested data," because "[i]f a party maintains electronic data for the purpose of utilizing it in connection

with current activities, it may be expected to respond to discovery requests at its own expense"); *with Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 321 (S.D.N.Y. 2003) (concluding that "'the purposes for which the responding party maintains the requested data' are typically unimportant," which suggests that using backup tapes for archival purposes may not adversely affect the cost-shifting analysis).

Organizations seeking to preserve data for business purposes or litigation should, if possible, consider employing means other than traditional disaster recovery backup tapes. *Cf.* 26 C.F.R. 1234.24(c) ("[B]ackup tapes should not be used for recordkeeping purposes.").

> *Illustration i.* Pursuant to an information technology management plan, once each day a producing party routinely copies all electronic information on its systems and retains, for a short period of time, the resulting backup tape for the purpose of reconstruction in the event of an accidental erasure, disaster or system malfunction. A requesting party seeks an order requiring the producing party to preserve, and to cease reuse of, all existing backup tapes pending discovery in the case. Complying with the requested order would impose large expenses and burdens on the producing party, which are documented in factual submissions. No credible evidence is shown establishing the likelihood that, absent the requested order, the producing party will not produce all relevant information during discovery. The producing party should be permitted to continue the routine recycling of backup tapes in light of the expense, burden and potential complexity of restoration and search of the backup tapes.

Finally, if it is unclear whether there is a reasonable likelihood that unique, relevant data is contained on backup tapes, the parties and or the court may consider the use of sampling to better understand the data at issue. *See McPeek v. Ashcroft*, 212 F.R.D. 33, 36 (D.D.C. 2003) (declining to order searches of backup tapes where plaintiff had not demonstrated a likelihood of obtaining relevant information after review of sample; *cf. Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003) (using sampling to determine that other backup tapes likely contained relevant data that should be produced). Depending on the circumstances of the case, sampling may establish that there are few, if any, unique documents on the tapes and that there is no need for the tapes to be retained or restored. Similarly, sampling techniques may establish that it is reasonable to retain and restore only certain intervals of available tapes (such as every tenth tape) to satisfy the party's good faith compliance with its preservation and production obligations. *See* Cmt. 11.c, *infra*.

Comment 5.i. Potential Preservation of Shared Data

An organization's networks or intranet may contain shared areas (such as public folders, discussion databases and shared network folders) that are not regarded as belonging to any specific employee. Such areas containing potentially relevant data should be identified promptly and appropriate steps taken to preserve shared data that is relevant.

If an organization maintains archival data on tape or other offline media not accessible to end users of computer systems, steps should promptly be taken to preserve those archival media that are reasonably likely to contain relevant information not present as active data on the organization's systems. These steps may include notifying persons responsible for managing archival systems to retain tapes or other media as appropriate.

6. Responding parties are best situated to evaluate the procedures, methodologies and technologies appropriate for preserving and producing their own electronic data and documents.

Comment 6.a. The Producing Party Should Determine the Best and Most Reasonable Way to Locate and Produce Relevant Documents in Discovery

It is the responsibility of the producing party to determine what is responsive to discovery demands and to make adequate arrangements to preserve and produce relevant information. *See Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243, 2003 WL 22410619, at *3 (S.D.N.Y. Oct. 22, 2003) (noting there are various ways to manage electronic documents and thus many ways in which a party may comply with its obligations); *cf. In re Ford Motor Co.*, 345 F.3d 1315 (11th Cir. 2003) (stating that the producing party's choice to review database and only produce those relevant portions was adequate discovery response absent specific evidence to the contrary). Failure to do so in an organized and methodical fashion has led some courts to impose penalties upon the top officers responsible. *See Danis v. USN Communications, Inc.,* No. 98 C 7482, 2000 WL 1694325, at *37 (N.D. Ill. Oct. 20, 2000) (listing elements of notification of discovery obligations not put into place).

Typically, the producing party identifies and informs the key individuals likely to have relevant information of the specific need to preserve all available relevant information. (This instruction is sometimes referred to as a "litigation hold order."). *See* Cmt. 5.d, *supra*. Thereafter, reasonable steps are taken to facilitate production of documents, after review for privilege, trade secrets, or other appropriate bases for non-production.

There is no principled reason to require more intrusive efforts merely because the party seeking discovery is suspicious of the efforts undertaken by the producing party. *See McCurdy Group, LLC v. American Biomedical Group, Inc.*, 9 Fed. Appx. 822, 831 (10th Cir. 2001) (affirming denial of motion to compel production of hard drives based on that party's expression of skepticism that all relevant and non-privileged documents had been produced).

Comment 6.b. Scope of Electronic Data Collection

When responding to discovery requests, organizations should define the scope of the data needed to appropriately and fairly address the issues in the case and to avoid unreasonable overbreadth, burden, and cost. Important steps in achieving the goal of reasonably limiting discovery may include collecting data from repositories used by key players rather than generally searching through the entire corporate computer system; defining the set of data to be collected by applying reasonable selection criteria, including search terms, date restrictions, or folder designations; and avoiding collection efforts that are out of proportion to or are inappropriate in the context of a particular litigation.

Discovery should not be permitted to continue indefinitely merely because a discovering party can point to undiscovered documents when there is no evidence that those documents are relevant to the case. *See Fennell v. First Step Designs, Ltd.*, 83 F.3d 526, 532-33 (1st Cir. 1996) (affirming order denying electronic discovery where that discovery would be a "fishing expedition"); *Stallings-Daniel v. Northern Trust Co.*, No. 01 C 2290, 2002 WL 385566, at *1 (N.D. Ill. Mar. 12, 2002) (refusing to reconsider denial of a request by plaintiff for an order permitting an expert to conduct an intrusive and detailed examination of discovery of defendant's e-mail system where the bases for the claims were "speculations").

> *Illustration i.* A party seeking access to e-mail relevant to the case demands that it be permitted to copy and inspect the active e-mail accounts of all users. The request should be denied. The producing party is in the best position to determine how to comply with its discovery obligations. Electronic information that is not deemed relevant should not be subject to inspection by the requesting party. The Rules do not create the right to a fishing expedition merely because the information sought is in electronic form. The concept of relevance is no broader—or narrower—in the electronic context than in the paper context.

Comment 6.c. Rule 34 Inspections

Rule 34 inspections should be the exception and not the rule for discovery of electronic data. Usually, the issues in litigation relate to the informational content of the data held on computer systems, not the actual operations of the systems. Therefore, in most cases, if the producing party provides the informational content of the data, there is no need or justification for direct inspection of the respondent's computer systems. A Rule 34 inspection presents possible concerns such as:

a) invading trade secrets;
b) revealing other highly confidential information, such as personnel evaluations and payroll information, properly private to individual employees;
c) encroaching upon confidential attorney-client communications and other confidential material prepared and organized by the party's attorneys;
d) massively disrupting the ongoing business; and
e) endangering the stability of operating systems, software applications, and electronic files if certain procedures or software are used inappropriately.

Further, Rule 34 inspections of electronic data are likely to be particularly ineffective. The standard form of production—in which the producing party identifies and produces responsive documents—allows the party with the greatest knowledge of the computer systems to search and utilize the systems to produce responsive documents. A Rule 34 inspection, in contrast, requires persons unfamiliar with the party's recordkeeping systems, hardware, and software to attempt to manipulate the systems.

Not only is such a process disruptive, it is less likely to be fruitful. Producing parties will most often be able to argue persuasively that their production of relevant information from computer systems and databases will be sufficient to discharge discovery obligations. *See In re Ford Motor Co.*, 345 F.3d 1315 (11th Cir. 2003) (vacating order allowing plaintiff direct access to defendant's databases).

To justify the onsite inspection of respondent's computer systems, a party should be required to demonstrate that there is a substantial need to discover information about the computer system and programs used (as opposed to the data stored on that system) and that there is no reasonable alternative to an onsite inspection. Any inspection procedure should be documented in an agreed upon (and/or court ordered) protocol and should be narrowly restricted to protect confidential information and system integrity and to avoid giving the discovering party access to data unrelated to the litigation.

Additionally, no inspection should be permitted to proceed until the producing party has had a fair opportunity to review the data subject to inspection. Where the requesting party makes the required showing to justify inspection of the other party's

systems, the data subject to inspection should be dealt with in a way to preserve the producing party's rights, for example, through the use of "neutral" court appointed consultants. *See* Cmt. 6.d and Illustration 9.b.ii, *infra*.

Comment 6.d. Use and Role of Consultants and Vendors

Responding parties may consider retaining consultants and vendors to assist them in preserving and producing their electronic data and documents. Due to the complexity of electronic discovery, many organizations rely on consultants to provide a variety of services, including helping plan discovery, performing specialized data processing, and engaging in forensic work. Such consultants can be of great assistance to parties and courts in providing technical expertise and experience with the collection, review, and production of electronic documents and data. *See also* Cmt. 10.c (Use of Special Masters and Court-Appointed Experts to Preserve Privilege).

However, standards for experts and consultants in this field have not yet fully developed. Parties and courts should carefully consider the experience and expertise of a potential consultant before his or her selection. Vendors offer a variety of software and services to assist with the electronic discovery process. Considerations in evaluating vendor software and services include the defensibility of the process in the litigation context, the cost, and the experience of the vendor.

At all times, counsel, clients, and vendors must understand the role of each in the discovery process. Thus, even if a vendor is retained to serve in a non-testifying role, everyone should be aware of the potential need for testimony if forensic or other technical expertise is applied to data to prepare it for review or production. Care should be taken to ensure that the vendor does not assume the role of a legal advisor, and all persons involved should understand which communications are protected under the attorney-client privilege, and which documents may be protected under a claim of attorney work product.

Comment 6.e. Documentation and Validation of Data Collection Procedures

In developing data collection procedures, organizations should consider the appropriate scope of the collection, the cost, burden and disruption of normal activities, and the defensibility of the process. All collection processes should be accompanied by documentation and validation appropriate to the needs of the particular case. Well-documented data collection and production procedures enable an organization to respond to challenges to the collection process and to avoid unintentionally collecting data that is not needed or overlooking data that should be collected.

The documentation should describe what is being collected, the procedures used and any steps used to validate the collection. This documentation should not be static but should be revised as the organization uses new or different technology.

Similarly, notice and instructions to end-users regarding collection of data should include clear descriptions of the information being sought; a reminder that the collection includes many types of electronic data; direction regarding where users should look for data; and the steps to follow in retrieving the data. Specifics will depend upon the organization's systems and the nature of the litigation.

7. The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronic data and documents were inadequate.

Comment 7.a. Rule 37 Sets Forth Guidelines for Resolving Discovery Disputes

A party that receives a request for production of electronic documents may object to some or all of the request. If such objections are filed and the requesting party opts not to accept the objections, the requesting party must file a motion to compel pursuant to Rule 37. *See, e.g., GFI Computer Indus., Inc. v. Fry*, 476 F.2d 1, 3 (5th Cir. 1973) ("Plaintiffs' remedy for incomplete or otherwise objectionable answers to interrogatories, and for failure to produce pursuant to a Rule 34 request, was to file a motion under Rule 37(a) for an order requiring defendant to answer and to produce documents for inspection.").

In such a proceeding, the moving party has the burden of demonstrating that the responding party's response to the discovery request, including its steps to preserve and produce electronic data and documents, was incomplete, and that additional efforts are warranted.

Comment 7.b. Discovery Against Third Parties Under Rule 45

The requesting party sometimes requests the same or similar materials from third parties under Rule 45 of the Federal Rules. In such cases, courts should balance the cost, burden, and need for imposing discovery burdens on third parties who may possess copies of such documents. *See Braxton v. Farmer's Ins. Group*, 209 F.R.D. 651, 653 (N.D. Ala. 2002) (court quashed non-party subpoena for all documents, including e-mail and electronic documents, from insurance agents where insurance company defendant alleged it was able to produce materials (including e-mails) it had sent to agents and the discovering party failed to make a showing that the insurer's production would be inadequate).

Requesting parties should be sensitive to the burdens that third-party discovery places on third-parties. Excessively broad electronic document production requests on third parties can lead to sanctions and liability under federal statutes protecting the privacy of electronic communications. *See Theofel v. Farey-Jones,* 341 F.3d 978 (9th Cir. 2003) (service of an overbroad, "patently unlawful" subpoena on a party's ISP, which led to the disclosure of private and privileged communications, violated the Stored Communications Act, 18 U.S.C. Section 2701 *et seq.*, and the Computer Fraud and Abuse Act, 18 U.S.C. Section 1030).

8. The primary source of electronic data and documents for production should be active data and information purposely stored in a manner that anticipates future business use and permits efficient searching and retrieval. Resort to disaster recovery backup tapes and other sources of data and documents requires the requesting party to demonstrate need and relevance that outweigh the cost, burden, and disruption of retrieving and processing the data from such sources.

Comment 8.a. Scope of Search for Active and Purposely Stored Data

The scope of a search for relevant electronic data and documents must be reasonable. For example, potentially relevant information may be found in local and network computers, laptop computers, handheld storage devices (such as PDAs and flash memory drives), archive and backup data tapes, cellular phones, voice mail systems and closed-circuit television monitoring systems.

However, it is neither feasible nor reasonable to require that litigants immediately or always canvass all potential reservoirs of data in responding to preservation obligations and discovery requests. Many of the locations will contain redundant data, and many others may contain massive amounts of information not relevant to the claims and defenses in the case.

Accordingly, litigants and courts must exercise judgment, made upon reasonable inquiry and in good faith, regarding the active and purposely stored data locations that should be subject to preservation efforts. If the producing party is aware (or reasonably should be aware) that specific relevant information can only be obtained from a particular source, that data should be preserved for possible production absent agreement of the parties or order of the Court.

If potentially relevant documents exist in sources that are not in a "readily usable" format, cost-shifting may be most appropriate. *See Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 319-20 (S.D.N.Y. 2003); Principle 13, *infra*.

Comment 8.b. Forensic Data Collection

Discovery should be limited to electronic data and documents that are relevant to the claims and defenses in the case. A requesting party should not be permitted to discover electronic data and documents that do not meet this standard, regardless of the technical feasibility of broader access.

Forensic data collection should not be required unless exceptional circumstances warrant the extraordinary cost and burden of such an approach. *See McPeek v. Ashcroft*, 212 F.R.D. 33, 36 (D.D.C. 2003) (declining to order searches of backup tapes where plaintiff had not demonstrated a likelihood of obtaining relevant information). However, a party could choose to meet certain preservation obligations by making or retaining copies of backup tapes. *Cf. Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243, 2003 WL 22410619, at *3 (S.D.N.Y. Oct. 22, 2003) (noting possible use of "mirror-image" copies in conjunction with other steps to meet preservation obligations). In some cases, such copies may best preserve all possibly relevant data.[16] In any event, making forensic image backups of computers is only the first step of an expensive, complex, and difficult process of data analysis that can divert litigation into side issues involving the interpretation of ambiguous forensic evidence.

Comment 8.c. Outsourcing Vendors and Third Party Custodians of Data

Many organizations outsource all or part of their information technology systems or share data with third parties for processing or for other business purposes. In contracting for such services, organizations should consider how they will comply with their obligations to preserve and collect electronic data for litigation. If such activities are not within the scope of contractual agreements, costs may escalate and necessary services may be unavailable when needed. Parties also need to consider whether notice should be sent to third parties, such as contractors and vendors. This concern arises out of FED. R. CIV. P. 34, which allows discovery of documents in the possession, custody or control of a party.

9. Absent a showing of special need and relevance, a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual data or documents.

Comment 9.a. The Scope of Document Discovery under the Federal Rules

Although FED. R. CIV. P. 34 was amended in 1970 to add "data compilations" to the list of discoverable documents, there was no suggestion that "data compilations" was intended to turn *all* forms of "data" into a Rule 34 "document." *Cf.* Shira A. Scheindlin &

16 For example, forensic copies of hard drives may be useful where key employees leave employment under suspicious circumstances, or if theft or misappropriation of trade secrets or confidential information may be involved.

Jeffrey Rabkin, *Electronic Discovery In Federal Civil Litigation: Is Rule 34 Up To The Task*?, 41 B.C. L. Rev. 327, 372 (2000) ("Embedded data, Web caches, history, temporary, cookie and backup files—all of which are forms of electronically stored information automatically created by computer programs rather than by computer users—do not obviously fall within the scope of the term 'documents'.").

The best approach to understanding what is a document is to examine what information is readily available to the computer user in the ordinary course of business. If the employee can view the information, it should be treated as the equivalent of a paper "document." Data that can be readily compiled into viewable information, whether presented on the screen or printed on paper, is also a "document" under Rule 34. However, data used by a computer system but hidden and never revealed to the user in the ordinary course of business should not be presumptively treated as a part of the "document," although there are circumstances in which the data may be relevant and should be preserved and produced. *See* Cmt. 12.a, *infra*. Nor should data, such as deleted or residual data, that is not accessible except through forensic means be presumed to be a document that is discoverable in all circumstances. Such data may be discoverable under Rule 34, but the evaluation of the need for and relevance of such discovery should be separately analyzed on a case-by-case basis. *See, e.g., McPeek v. Ashcroft,* 202 F.R.D. 31, 33 (D.D.C. 2001) (court rejected notion that there is an absolute obligation to pursue potentially relevant data on backup tapes); *McPeek v. Ashcroft*, 212 F.R.D. 33, 35-37 (D.D.C. 2003) (rejecting 15 out of 16 of plaintiff's demands for additional searches of backup tapes). At least one state court system—that of Texas—has adopted this viewpoint and created a presumption that heroic efforts to produce data are not ordinarily required. *See* Texas R. Civ. P. 196.4 ("The responding party must produce the electronic or magnetic data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business. If the responding party cannot—through reasonable efforts—retrieve the data or information requested or produce it in the form requested, the responding party must state an objection complying with these rules."); Cmt. 5.e, *supra*.

> *Illustration i.* A party demands that responsive documents, "whether in hard copy or electronic format," be produced. The producing party objects to producing the documents in electronic format and states that production will be made through PDF or TIF images on CD-ROMs. The producing party assembles copies of the relevant hard copy memoranda, prints out copies of relevant e-mails and electronic memoranda, and produces them in a PDF or TIF format that does not include metadata. Absent a special request for metadata (or any reasonable basis to conclude the metadata was relevant to the claims and defenses in the litigation), and a prior order of the court based on a showing of need, this production of documents complies with the ordinary meaning of Rule 34.
>
> *Illustration ii.* Plaintiff claims that he is entitled to a commission on a transaction, based upon an e-mail allegedly sent by the president of defendant corporation agreeing to the commission. Defendant asserts that there is no record of the e-mail being sent in its e-mail system or the logs of its Internet activity, and that the e-mail is not authentic. In these circumstances, it is appropriate to require production of not only the content of the questioned e-mail, but also of the e-mail header information and metadata, which can play a crucial role in determining whether the questioned message is authentic.

> *Illustration iii.* Plaintiff alleges that the defendant engaged in a fraud regarding software development. The plaintiff shows that the computer program sold by defendant appears to incorporate plaintiff's source code. Plaintiff presents two copies of a letter allegedly sent on the same day to plaintiff, but the letters differ in a material manner. In this case, discovery of the source code data may be appropriate, as well as targeted discovery of any electronic drafts or metadata concerning the suspect letter.

Comment 9.b. Deleted Data and Residual Data

Absent specific circumstances, organizations should not have to preserve deleted or residual data. While most computer systems will have a plethora of data that could be "mined," there should not be routine authorization for such forensic recovery. If, as usual, deleted and residual data are not accessed by employees in the ordinary course of business, there is no reason to require the routine preservation of such data. The relevance of the data will be marginal at best in most cases, while the burdens involved will usually be great. In exceptional cases, however, there may be good cause for targeted preservation of deleted and residual data.[17]

Deleted and residual data, like papers discarded in the trash, may be subject to discovery and may even properly be described as a document under Rule 34. *See Antioch Co. v. Scrapbook Borders, Inc.,* 210 F.R.D. 645, 652 (D. Minn. 2002) ("[I]t is a well accepted proposition that deleted computer files, whether they be e-mails or otherwise, are discoverable."); *Rowe Entm't, Inc. v. The William Morris Agency, Inc.,* 205 F.R.D. 421, 428 (S.D.N.Y. 2002) (stating that "[e]lectronic documents are no less subject to disclosure than paper records);" *Simon Prop. Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 640 (S.D. Ind. 2000) ("[C]omputer records, including records that have been 'deleted', are documents discoverable under FED. R. CIV. P. 34."). Thus, even if production of deleted or residual data is unwarranted, parties should communicate early about the possible relevance of deleted data in order to avoid costly and unnecessary preservation of deleted or residual data, on one hand, or claims of spoliation, on the other.

However, only exceptional cases will turn on "deleted" or "discarded" information (whether paper or electronic). Discovery efforts, agreements, and orders of the courts should reflect this fact. *See Concord Boat Corp. v. Brunswick Corp.*, No. LR-C-95-781, 1997 WL 33352759, at *9 (E.D. Ark. Aug. 29, 1997) ("Fourteen days worth of e-mail, which might contain a few deleted e-mails, seems to hardly justify the expense necessary to obtain it. Similarly, even if earlier back up tapes containing 'snapshots' of the system were in existence, the potential limited gains from a search of such tapes would be outweighed by the substantial burden and expense of conducting the search. Accordingly, the Court finds that Defendant will not be required to restore and search any available back up tapes which might contain deleted [ ] e-mail]."). *But see Munshani v. Signal Lake Venture Fund II, LP,* 13 Mass. L. Rptr. 732, No. 005529BLS, 2001 WL 1526954, at *3-4 (Mass. Super. Ct. Oct. 9, 2001) (allowing use of court-appointed forensic consultant and determining that plaintiff had fabricated electronic documents based on testimony of that expert).

> *Illustration i.* A party seeking relevant e-mails demands a search of inactive accounts, backup tapes, and hard drives for deleted materials. No showing

17 Deleted data may at one time have been a "useful" document generated in the ordinary course of business that had value to the organization, although that value may have expired. However, this historic fact alone does not justify the retrieval and review of deleted or residual data. Absent specific evidence to the contrary, a presumption of regularity should apply that allows employees and organizations to properly and routinely delete or destroy documents that no longer have business value, so long as the documents are not subject to regulatory, investigatory or litigation preservation obligations.

of special need or justification is made for the extraordinary search. The request should be denied. Parties are not typically required to sequester and search the trash bin outside an office building after commencement of litigation; neither should they be required to preserve and produce deleted electronic information in the normal case.

Illustration ii. After a key employee leaves X Company ("X Co.") to work for a competitor, a suspiciously similar competitive product suddenly emerges from the new company. X Co. produces credible testimony that the former employee bragged about sending confidential design specifications to his new company computer, copying the data to a CD, and deleting the data so that the evidence would never be found. The court properly orders that, given the circumstances of the case, the requesting party has demonstrated the need for the computer to be produced for mirror image copying of its hard drive. If the defendant is not willing to undertake the expense of hiring its own reputable data recovery expert to produce all available relevant data, inspection of the computer's contents by an expert working on behalf of X Co. may be justified, subject to appropriate orders to preserve privacy, to protect data, and to prevent production of unrelated or privileged material. Under a showing of special need, with appropriate orders of protection, extraordinary efforts to restore electronic information could also be ordered.

10. A responding party should follow reasonable procedures to protect privileges and objections to production of electronic data and documents.

Comment 10.a. Potential Waiver of Confidentiality and Privilege in Production

Because of the large volumes of documents and data typically involved when electronic data is produced, courts should consider entering orders protecting the parties against any waiver of privileges or protections due to the inadvertent production of documents and data.

Counsel should discuss the need for such a provision at the outset of litigation and should approach the court for entry of an appropriate non-waiver order.[18] Such an order should provide that the inadvertent disclosure of a privileged document does not constitute a waiver of privilege, that the privileged document should be returned (or there will be a certification that it has been deleted), and that any notes or copies will be destroyed or deleted.[19] Ideally, an agreement or order should be obtained before any production.

18 The recently issued proposed amendments to the ABA Civil Discovery Standards reflect this recommendation. *See* Nov. 17, 2003 proposed *ABA Civil Discovery Standards* at Section 32(b).

19 An example is in the Bridgestone/Firestone/Ford multi-district litigation from the Southern District of Indiana. The pertinent provision of the Case Management Order states:

> In the event that a privileged document is inadvertently produced by any party to this proceeding, the party may request that the document be returned. In the event that such a request is made, all parties to the litigation and their counsel shall promptly return all copies of the document in their possession, custody, or control to the producing party and shall not retain or make any [copies]. Such inadvertent disclosure of a privileged document shall not be deemed a waiver with respect to that document or other documents involving similar subject matter.

In re Bridgestone/Firestone, Inc., ATX, ATX II, and Wilderness Tires Prods. Liab. Litig., 129 F. Supp. 2d 1207, 1219 (S.D. Ind. 2001). Other courts prefer that such orders include a temporal qualification on the right to assert a claim of inadvertent production (*i.e.*, within a "reasonable time" or a "date certain" from production) as well as a qualification that the producing party must state that it employed good faith efforts to detect and prevent production of privileged or protected materials and that the document in question was inadvertently produced notwithstanding such efforts. The inclusion of such additional conditions may vary between jurisdictions and will likely depend on the anticipated magnitude of the production in the case.

Comment 10.b. Protection of Confidentiality and Privilege Regarding Rule 34 Inspections

Special issues may arise with any request to inspect a computer system. Protective orders should be in place to guard against any release of proprietary, confidential information and protected personal data if a system is reviewed by the adversary or its expert.

Similar concerns exist regarding the potential disclosure of attorney-client privileged or work product information. There is no guarantee that a non-waiver order in one jurisdiction will be fully honored in another if protected information is disclosed. Accordingly, court-ordered inspections of computer systems should be used sparingly. Further, such orders should be narrowly tailored to the circumstances and accompanied by a sufficient protective order.

Comment 10.c. Use of Special Masters and Court-Appointed Experts to Preserve Privilege

In certain circumstances, a court may find it beneficial to appoint a "neutral" person (*e.g.*, a special master or court-appointed expert) who can help mediate or manage electronic discovery issues. *See Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 652-54 (D. Minn. 2002) (granting motion to appoint "neutral expert in computer forensics"); *Simon Prop. Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 641-42 (S.D. Ind. 2000) (using appointed expert operating under constraints of protective order); *Dodge, Warren & Peters Ins. Servs., Inc.*, 105 Cal. App. 4th 1414, 1417, 130 Cal. Rptr. 385 (4 Dist. 2003) (affirming order that allowed inspection by court-appointed expert).

The December 1, 2003 amendment to Rule 53 (Special Masters) should help clarify the availability of special masters to federal courts for addressing electronic discovery issues in appropriate cases where the matters cannot be addressed effectively and timely by an available district judge or magistrate judge of the district. *See* FED. R. CIV. P. 53(a)(1)(C).

One immediate benefit of using such a court-appointed "neutral" third party is the probable elimination of privilege waiver concerns with respect to the review of information by that person. In addition, the "neutral" may be able to speed the resolution of disputes by fashioning fair and reasonable discovery plans based upon specialized knowledge of electronic discovery and/or technical issues with access to specific facts in the case.[20] *See id.*

Special care should be used in crafting the order of appointment (and any protective order) to precisely tailor the scope of appointment and protections against the disclosure or loss of any privileges or protections. It should also be noted such appointments likely will remain the exception and not the rule as most parties, through the disclosure and discovery process should be able to address electronic discovery issues and remaining disputes often can be decided by an available district court or magistrate judge of the district.

Comment 10.d. Protection of Confidentiality and Privilege Regarding "Clawback" or "Quick Peek" Productions

Given the enormous volume of electronic documents generated and retained in today's business environment, and in light of the demands of litigation, there is an increasing interest in production subject to so-called "clawback" agreements. *See, e.g., Zubulake v. UBS Warburg LLC,* 216 F.R.D. 280, 290 (S.D.N.Y. 2003) ("*Zubulake III*") ("Indeed, many

20 The proposed amendments to the ABA Civil Discovery Standards reflect this same notion. *See* Nov. 17, 2003 proposed *ABA Civil Discovery Standards* at Section 32(a), (c) and (e).

parties to document-intensive litigation enter into so-called 'claw-back' agreements that allow the parties to forego privilege review altogether in favor of an agreement to return inadvertently produced privileged documents.").

In a "clawback" (or "quick peek") production, documents are produced to the opposing party before or without a review for privilege, confidentiality, or privacy. The key component of such a production is the "clawback" agreement, in which the parties set stringent guidelines and restrictions to prevent the waiver of confidentiality and privilege. The assumption of the parties to such a "clawback" agreement is that if the requesting party finds a document that appears to be privileged, the producing party can "claw back" the document without having waived any privilege.

A "clawback" or "quick peek" procedure or order in civil litigation should not be lightly entered and should have the voluntary consent of the producing party. *See Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, No. Civ. A. 99-3564, 2002 WL 246439, at *7 (E.D. La. Feb. 19, 2002) (noting that court cannot compel the disclosure of privileged communications in clawback arrangement). Despite the apparent advantage of reducing the costs of pre-production reviews for privilege and confidentiality (and maybe even responsiveness), there are a host of risks and problems that make "clawback" productions impracticable and, for most cases, ill-advised.

First, the voluntary production of privileged and confidential materials to one's adversary, even in a restricted setting, is inconsistent with tenets of privilege law that, while varying among jurisdictions, usually require the producing party to meticulously guard against the loss of secrecy for such materials. *See In re Sealed Case*, 877 F.2d 976, 980 (D.C. Cir. 1989) (nearly any disclosure of the communication or document, even inadvertent, waives the privilege); *cf. Fleet Bus. Credit Corp. v. Hill City Oil Co.*, No. 01-02417, 2002 WL 31741282, at *9-11 (W.D. Tenn. Dec. 5, 2002) (applying a number of factors to determine if inadvertent disclosure waived privilege and concluding that reviewing documents for privilege before disclosure, and then acting swiftly to correct inadvertent disclosure, preserved privilege). Thus, the fact that an adversary sees the voluntarily produced document in any circumstance may be argued to trigger the waiver or loss of protection.

Second, despite the strongest possible language in any "clawback" or "quick peek" order to protect against waiver of privileges and dissemination of information, there is no effective way to limit the arguments of non-parties regarding the legal effect of the production in other jurisdictions and forums. For example, parties in mass tort and product liability cases, who are subject to multiple suits by different counsel in different states, face the reality that their clawback agreement does not protect them from waiver arguments in another state, even if they have a strong protective order in the first state. Given the differences in of privilege laws among jurisdictions, this uncertainly presents a serious and legitimate impediment to any widespread acceptance of a "clawback" model.

Third, counsel has an ethical duty to zealously guard the confidences and secrets of the client. It is possible that questions could arise as to whether voluntarily entering into a "clawback" production could constitute a violation of Model Rules of Professional Conduct 1.1 (requiring a lawyer to use diligence and care in representation) or Model Rules of Professional Conduct 1.6 (protection of client secrets and confidences) if the manner of the production results in later waivers of privileges and protections. While this result may seem remote, it has already arisen in the content of inadvertent productions. *See* D.C. Bar Ethics Opinion No. 256 (1995) (examining whether actions of producing counsel violated standard).

Fourth, there is a Pandora's box of issues regarding the possible rights of employees (privacy) and third parties (privacy and commercial trade secrets) that may be implicated in a voluntary "clawback" or "quick peek" production.

Given these concerns, and the due process issues attendant to the potential deprivation of privilege and property rights that could accompany a waiver determination, courts should not compel use of a "clawback" procedure over the objection of a producing party. Even when large volumes of electronic documents are involved, parties are well-advised to search for privileged documents[21] before production, while obtaining a court order that inadvertent production of privileged material does not waive privilege. *See, e.g., Medtronic Sofamor Danek, Inc. v. Michelson*, No. 01-2373, 2003 WL 21468573, at *12 (W.D. Tenn. May 13, 2003).

In those very limited instances where a "clawback" or "quick peek" order may be practicable, the Court should enter an order that (1) indicates that the court is compelling the manner of production, (2) states such production does not result in an express or implied waiver of any privilege or protection for the produced documents or any other documents, (3) directs that the reviewing party cannot discuss the contents of the documents or take any notes during the review process, (4) permits the reviewing party to select those documents that it believes are relevant to the case, and (5) orders that for each selected document, the producing party either (a) produces the selected document, (b) places the selected document on a privilege log, or (c) places the selected document on a non-responsive log (i.e., regardless of the privileged status, the document is not relevant to the litigation.) *Cf. Murphy Oil,* No. Civ. A. 99-3564, 2002 WL 246439, at *12 (outlining clawback protocol).[22]

11. A responding party may satisfy its good faith obligation to preserve and produce potentially responsive electronic data and documents by using electronic tools and processes, such as data sampling, searching, or the use of selection criteria, to identify data most likely to contain responsive information.

Comment 11.a. Search Methodology

In many cases, electronic data are found in broadly categorized folders such as an e-mail "inbox" or "outbox", or are otherwise not archived in a manner that can be used to readily identify responsive information. For example, selective use of key "concept" or word searches is a reasonable approach when dealing with large amounts of electronic data. Indeed, a principal advantage of electronic information is that high-speed methods exist to determine the existence of patterns of words, thereby allowing the narrowing of searches for relevant information. *See Lombardo v. Broadway Stores, Inc.*, 2002 WL 86810, at *8 (Cal. App. Jan. 22, 2002) ("Broadway urges the hard copy payroll documents were the same as the computerized data. Not so. The hard copy may have contained the same information, but that information was not equally accessible.").

In appropriate circumstances, litigants may find it useful to discuss specific selection criteria, including search terms, to be used in searches of electronic data for production. Parties may be able to begin a dialogue on search methodologies as early as their Rule 26(f) conference.

---

21 The search methods discussed in Principle 11, *infra*, in relation to searches for relevant documents may be useful to identify privileged documents as well.

22 The proposed amendments to the ABA Civil Discovery Standards identify the "clawback" or "quick peek" alternative as a possible provision for a stipulated court order but do not discuss situations where it would be advisable, privilege waiver questions pertaining to other jurisdictions, whether a court could direct the procedure over an objection, or the other protections listed above in the event the parties stipulated to such an order. *See* Nov. 17, 2003 proposed *ABA Civil Discovery Standards* at Section 32(d)(ii) and (f).

Courts should encourage and promote the use of such techniques in appropriate circumstances. *See Tulip Computers Int'l B.V. v. Dell Computer Corp.*, No. Civ. A. 00-981, 2002 WL 818061, at *4 (D. Del. Apr. 30, 2002) ("Tulip's consultant will search the CD ROM on certain mutually agreed upon search terms that relate to the infringing products or to this case. Such terms may involve 'Tulip' or code words for the allegedly infringing models such as 'STINGER,' 'MASH,' or 'HONEYCUT.' If the search terms generate hits, Dell will review the documents and produce them to Tulip subject to the privilege and confidentiality designations provided under the protective order.").

Courts can allow sampling techniques to refine the accuracy of searches and to reduce the cost of discovery. *See McPeek v. Ashcroft*, 202 F.R.D. 31, 34-35 (D.D.C. 2001). For example, sampling might determine that a very low percentage of files (such as e-mails and attachments) on a data tape contain terms that are responsive to "key" terms. This may weigh heavily against any need to further search that source, or it may be a factor in a cost shifting analysis. Sampling may also reveal substantial redundancy between sources (*i.e.*, duplicate data is found in both locations) such that it is reasonable for the organization to preserve and produce data from only one of the sources. *See* Cmt. 11.c, *infra*.

The scope of terms employed must be reasonably calculated to return relevant data. If not, courts may order additional searches, which will increase the cost and burden of discovery. For example, in *In re Amsted Industries, Inc. "Erisa" Litig.*, 2002 WL 31844956, at *2 (N.D. Ill. Dec. 18, 2002), the court found that the defendants' document production efforts, which involved word searches on 25 backup tapes of e-mail and the questioning of individuals regarding e-mails on their computers, were insufficient, and that additional searches not limited by defendants' relevancy objections were required.

> *Illustration i.* The active e-mail accounts of the individuals likely to have information relevant to litigation contain 10,000 individual e-mails from the relevant time period. Rather than read each one, the producing party uses a series of search terms that capture the key concepts in the allegations of the complaint. The producing party has satisfied its search obligations.

Comment 11.b. Sampling

Litigants should consider the use of sampling techniques when appropriate to narrow the burden of searching voluminous electronic data for relevant information. By reviewing an appropriate sample of a large body of electronic information, litigants can often determine the likelihood that a more comprehensive review of the materials will yield useful information.

For example, in *McPeek v. Ashcroft,* 202 F.R.D. 31 (D.D.C. 2001), Magistrate Judge Facciola ordered the "backup restoration of the e-mails attributable to" a particular individual's computer during a one-year period. *Id.* at 34. Judge Facciola viewed this restoration as "a test run," *id.*, which would allow the court and the parties to better determine whether a further search of the backup tapes was justified. Upon reviewing the results of the sample restoration, Judge Facciola held that further restoration of backup tapes was largely unjustified, and ordered very limited discovery of e-mails contained on backup tapes. *See McPeek v. Ashcroft*, 212 F.R.D. 33, 37 (D.D.C. 2003); *see also Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 324 (S.D.N.Y. 2003) ("Requiring the responding party to restore and produce responsive documents from a small sample of backup tapes will inform the cost-shifting analysis.").

Comment 11.c. Consistency of Manual and Automated Collection Procedures

Both manual and automated procedures for collection may be appropriate in particular situations. Whether manual or automated, the procedures must be directed by legal counsel to assure compliance with discovery obligations.

Manual collection involves selecting items that are potentially relevant to a given litigation. This selection can be performed by the document authors or custodians themselves, by litigation support or information services personnel, or by others. In a manual collection, the items may be copied or transmitted by the end-user. This should be accomplished under a defined protocol.

Automated collection involves using computerized processes to collect data meeting certain criteria, such as search terms, file and message dates, or folder locations. Automated collection can be integrated with an overall electronic data archiving or retention system, or it can be implemented using agents specifically designed to retrieve information on a case-by-case basis. Regardless of the method chosen, consistency across the production can help ensure that responsive documents have been produced as appropriate.

12. Unless the producing party knows that particular metadata is material to the resolution of a dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court.

Comment 12.a. Metadata

An electronic document usually includes not only the visible text but also hidden text, formatting codes, formulae, and purposefully generated metadata associated with the document. Much of it can be described as data that tells the computer how to display the document (for example, the proper fonts, spacing, size and color). Depending on the circumstances of the case, particular metadata may be critical or completely irrelevant.

Other embedded data reflects information intentionally created by the user or by the organization's information management system. Such information may, for example, track the title of the document, the user identification of the computer that created it, the assigned data owner, and other document "profile" information. Often this information is not significant to the resolution of a dispute, but there are situations where it may be important.

When a document is printed (or saved in an image format), much of the "display" of the document is preserved, but not the hidden metadata. Some of the metadata existing in a computer file can be routinely accessed by users; other metadata is not routinely accessible. Sometimes the metadata is inaccurate, as when a form document reflects a standard "author" who created the template but did not draft the document.

Although there are exceptions to every rule, especially in an evolving area of the law, there should be a modest legal presumption in most cases that the producing party need not take special efforts to preserve or produce metadata.[23] It is likely to remain the exceptional situation in

23 The vitality of this presumption is reflected in the D.C. Circuit Court of Appeals' opinion in *Pub. Citizen v. Carlin*, 184 F.3d 900, 908-11 (D.C. Cir. 1999), *cert. denied*, 529 U.S. 1003 (2000). The plaintiffs there challenged the Archivist of the United States' promulgation of a General Records Schedule which allowed the disposal of word processing and electronic mail files located in personal computers once they were copied to a paper or electronic recordkeeping system. *Inter alia*, the plaintiffs argued that the "print and retain" option obliterated valuable metadata which improperly diminished the value of the records in question. The Court of Appeals rejected these arguments and, in reversing the district court, held that the value of electronic retention must be balanced against the feasibility of doing so, the funds and resources available for records management, and the operating needs of the custodial agencies. *Id.* at 910 ("… we think [the Archivist's] decision to permit agencies to maintain their recordkeeping systems in the form most appropriate to the business of the agency is reasonable. [There is no] claim that agencies have a legal duty to establish electronic recordkeeping systems."). The court also noted that the Archivist interpreted the regulation to require the retention of information preserving the "context, structure and context" of the record (*i.e.*, material information) and there was no reason to conclude the Archivist's view was plainly erroneous. *Id.* at 910-11.

which metadata must be produced. *See, e.g., Munshani v. Signal Lake Venture Fund II, LP*, 13 Mass. L. Rptr. 732, No. 005529BLS, 2001 WL 1526954, at *3-4 (Mass. Super. Ct. Oct. 9, 2001) (court found that plaintiff had fabricated documents based upon testimony of court-appointed forensic consultant who revealed fraud in creation of proffered e-mail evidence).[24]

Notwithstanding this legal presumption, the routine preservation and production of metadata may be beneficial in a number of ways. First, the preservation and production of metadata may provide better protection against inadvertent or deliberate modification of evidence by others. Second, preserving documents in their native electronic format usually preserves the associated metadata without incurring additional steps or costs. Third, the systematic removal or deletion of certain metadata may involve significant additional costs that are not justified by any tangible benefit. Fourth, the failure to preserve and produce metadata may deprive the producing party of the opportunity to later contest the authenticity of the document if the metadata would be material to that determination.

Balanced against these factors is the reality that most of the metadata has no evidentiary value, and any time (and money) spent reviewing it is a waste of resources. However, since certain metadata could contain or reveal privileged, secret, or other sensitive information, an organization may determine that it must review such metadata before producing it.

Thus, a reasonable balance is that, unless the producing party is aware (or should reasonably be aware) that particular metadata is relevant, the producing party should have the option of producing all, some or none of the metadata.[25] In most cases, responding parties will reasonably choose to produce some or all of the metadata because of potential relevance or cost considerations. Of course, if the producing party knows or should reasonably know that particular metadata is relevant to the dispute, it should be produced.

In short, litigants and courts need to scrutinize the claims and defenses before determining how to handle metadata. Organizations should not automatically discount the potential benefits of retaining metadata to ensure the documents are authentic and to preclude the fraudulent creation of evidence. Finally, parties should consider discussing at the outset of litigation the need to preserve and produce metadata.

Comment 12.b. Formats Used for Collecting Data

The appropriate format for collection should be determined after considering the nature of the litigation. Parties should carefully consider whether converting electronic documents to other formats would impose unnecessary costs on the producing party. Also, because electronic data (*e.g.*, metadata) can sometimes be altered by converting formats or by copying the data, parties should document their process of collecting and producing electronic documents to ensure that the documents can later be authenticated if needed at trial.

---

24 Much of the information that can be retrieved from metadata is less relevant and necessary than the information that can be retrieved from paper documents. For example, certain metadata, such as metadata reflecting prior revisions to a document, can be analogized to paper drafts. There is authority supporting the proposition that paper drafts are rarely needed to prove the point in contention. Indeed, one court (speaking in the paper context) noted:

> Drafts, by their very nature, rarely satisfy the test of relevance … Absent extrinsic evidence tending to show the relevance of a particular draft, production of these documents is likely to lead only to wasteful fishing expeditions concerning the identification and deciphering of handwriting and the reasons for immaterial revisions.

Grossman v. Schwarz, 125 F.R.D. 376, 385 (S.D.N.Y. 1989).

25 *Cf.* John C. Montaña, *Legal Obstacles to E-Mail Destruction* at 32 (ARMA International Education Foundation, Oct. 19, 2003) ("In view of the fact that courts in [various] jurisdictions are prepared to accept printouts into evidence, and that the governments themselves view printout-based e-mail retention as a legitimate means of carrying out their mandated records management duties, it appears that, unless a specific legal requirement with a clear contrary indication applies, paper-based retention of e-mail is an acceptable course of action.").

Comment 12.c. Production of Electronic Data and Documents Should Only be Required in One Format

Electronic data should be produced in a form that preserves the substantive information of the data relevant to the claims and defenses in the action. Ordinarily parties should only be required to produce documents in one format.

Absent specific objection, agreement of the parties, or order of the court, producing electronic data in a commonly accepted image format (paper, PDF, or TIF) should be sufficient in most cases.[26] Similarly, absent specific objection, agreement of the parties or order of the court, data that is not ordinarily viewable when normally printed need not be produced. In certain cases, it may be preferable and more cost-effective to produce in an electronic format.

Often the parties will be able to agree upon a format of production during their Rule 26 conference. Sometimes the requesting party will specify the format it seeks in its Rule 34 request for production of documents. In such cases, the responding party may produce the documents in the requested format or may lodge an objection under the Federal Rules of Civil Procedure. It is best for the requesting party to identify at the outset a preferred manner of production so that agreement can be reached or so that disputes can be adjudicated before production. The format chosen should allow the parties to verify the genuineness and authenticity of the documents for evidentiary purposes.

A party should not be required to produce documents in both hard copy and electronic format. *See, e.g., McNally Tunneling Corp. v. City of Evanston*, No. 00 C 6979, 2001 WL 1568879, at *4 (N.D. Ill. Dec. 10, 2001) (denying motion to compel production of computer files that had already been produced in hard copy form where requesting party only offered vague assertions supporting its need for electronic version); *Williams v. Owens-Illinois, Inc.*, 665 F.2d 918, 932-33 (9th Cir. 1982) (same). *But see Anti-Monopoly, Inc. v. Hasbro, Inc.*, No. 94 Civ. 2120, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995) ("[P]roduction of information in 'hard copy' documentary form does not preclude a party from receiving that same information in computerized/electronic form."). If a court requires production of documents a second time in a different format, the court should consider shifting the costs of production to the requesting party. *See In re Air Crash Disaster at Detroit Metro. Airport on August 16, 1987,* 130 F.R.D. 634, 636 (E.D. Mich. 1989) (requiring requesting party to bear costs of creating copies of data in electronic form).

13. Absent a specific objection, agreement of the parties or order of the court, the reasonable costs of retrieving and reviewing electronic information should be borne by the responding party, unless the information sought is not reasonably available to the responding party in the ordinary course of business. If the data or formatting of the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information should be shifted to the requesting party.

Comment 13.a. Factors for Cost-Shifting

The ordinary and predictable costs of discovery are fairly borne by the producing party. However, Rule 26(b) empowers courts to shift costs where the demand is unduly

26 It is important to remember that the vast majority of civil cases involve only a small amount of discovery and there is no good reason to require that all cases involve meticulous electronic discovery absent a particular need in specific circumstances. *Cf.* Thomas E. Willging, John Shapard, Donna Stienstra, & Dean Miletich, *Discovery and Disclosure Practice, Problems, and Proposals for Change: A Case-based National Survey of Counsel in Closed Federal Civil Cases* (Federal Judicial Center, 1997) (providing statistical analysis of use of discovery devices and frequency of disputes).

burdensome because of the nature of the effort involved to comply. If a court requires retrieval of information that is not reasonably available, it should also adjudicate the need for cost shifting. *See Rowe Entm't, Inc. v. The William Morris Agency, Inc.*, 205 F.R.D. 421, 431 (S.D.N.Y. 2002) ("[A] party that happens to retain vestigial data for no current business purposes, but only in case of an emergency or simply because it has neglected to discard it, should not be put to the expense of producing it.").

Absent special circumstances, costs of electronic discovery involving extraordinary effort or resources to restore data to an accessible format should be allocated to the requesting party. For example, restoring deleted data, disaster recovery tapes, residual data, or legacy systems may involve such extraordinary efforts or resources.

The *Rowe* court laid out eight factors to use in determining whether to shift the costs of discovery to the requesting party: the specificity of the requests, the likelihood of a successful search, the availability of the materials from other sources, the purpose of the retention, the benefit to the parties, the total costs, the ability to control costs, and the parties' resources. *See Rowe*, 205 F.R.D. at 429-31.

These factors provide a useful tool to enable courts and litigants to analyze the circumstances under which the expenses of discovery exceed those that a responding party should reasonably be expected to bear. *See also ABA Civil Discovery Standards*, Standard 29(b)(iii)(1999) ("The discovering party generally should bear any special expenses incurred by the responding party in producing requested electronic information.");[27] Texas R. Civ. P. 196.4 ("If the court orders the responding party to comply with the request [for materials not available to the responding party in the ordinary course of business], the court must also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information."); *Medtronic Sofamor Danek, Inc. v. Michelson*, No. 01-2373, 2003 WL 21468573, at *2-9 (W.D. Tenn. May 13, 2003) (applying Rowe factors); *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, No. Civ. A. 99-3564, 2002 WL 246439, at *5-8 (E.D. La. Feb. 19, 2002) (same).

The factors announced in *Rowe* were revised and refined by Judge Shira Scheindlin in *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) ("*Zubulake I*"). Judge Scheindlin began by holding that "whether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an *accessible* or *inaccessible* format." *Id.* at 318. Data is in an accessible format if it can be easily retrieved and processed. Such data includes active data, near-line data, and archival data. Data in an inaccessible format is "not readily usable." *Id.* at 318-19. Inaccessible data includes backup tapes and deleted, fragmented, or damaged data. For accessible data, cost-shifting is not appropriate. *Id.* at 319.

For inaccessible data, however, Judge Scheindlin concluded that a set of factors similar to those in Rowe should determine whether the court should shift costs to the requesting party. Those factors, in the order of importance, are:

1. The extent to which the request is specifically tailored to discover relevant information;
2. The availability of such information from other sources;
3. The total cost of production, compared to the amount in controversy;
4. The total cost of production, compared to the resources available to each party;
5. The relative ability of each party to control costs and its incentive to do so;

27 The proposed amendments to the ABA Civil Discovery Standards omit this guidance and instead set forth a list of factors to be considered. *See* Nov. 17, 2003 proposed *ABA Civil Discovery Standards* Section 29(b)(iii).

6. The importance of the issues at stake in the litigation; and
7. The relative benefits to the parties of obtaining the information.

Id. at 322. *Zubulake I* stands to become a major precedent in the law of the cost-shifting for electronic discovery.

There remains a significant open question as to whether the "total cost of production" factor should include the estimated costs of reviewing retrieved documents for privilege, confidentiality and privacy purposes. The *Zubulake III* decision (*Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003)) excludes the cost of production (*e.g.*, review for privilege) from consideration,[28] but Rule 26 does not so narrowly define the burdens that can be considered by a court in the proportionality analysis. The inclusion/exclusion of such figures can greatly affect the outcome of the balancing test and, in light of the broad considerations mandated in Rules 26(b)(2) and 26(c)[29] and the potentially enormous costs of privilege review of voluminous electronic materials, it may be appropriate to shift some of the privilege review costs to the requesting party in certain circumstances. *See Chimie v. PPG Indus. Inc.*, 218 F.R.D. 416, 421-22 & n.7 (D. Del. 2003) (court found that in circumstances of case "and despite the magnitude of the labor" it was necessary "for PPG to log all arguably relevant documents for which it claims privilege" covering a 20 year period but added that "[t]he costs associated with searching for documents over such an extended period are open to further discussion. It may be that some cost sharing is warranted.").

Comment 13.b. Cost-Shifting Cannot Replace Reasonable Limits on the Scope of Discovery

Shifting the costs of extraordinary efforts to preserve or produce electronic information should not be used as an alternative to sustaining a responding party's objection to undertaking such efforts in the first place. Instead, such efforts should only be required where the requesting party demonstrates substantial need or justification.

In shifting discovery costs, the courts should discourage burdensome requests that have no reasonable prospect, given the size of the case, of producing material assistance to the fact finder. *See Stallings-Daniel v. Northern Trust Co.*, No. 01 C 2290, 2002 WL 385566, at *1 (N.D. Ill. Mar. 12, 2002) (denying request for discovery where "[n]othing in the documents produced justifies an intrusive and wholly speculative electronic investigation into defendant's e-mail files.").

> *Illustration i.* A requesting party demands that the producing party preserve, restore, and search a backup tape for information about a topic in dispute. The requesting party produces some evidence that relevant information, not available elsewhere, may exist on the tape. The information, not being readily available, is costly to acquire and the

---

28 *Zubulake III*, 216 F.R.D. at 290 ("the responding party should always bear the cost of reviewing and producing electronic data once it has been converted to an accessible form"); *see also Computer Assocs. Int'l, Inc. v. Quest Software, Inc.*, No. 02 C 4721, 2003 WL 21277129, at *2 (N.D. Ill. June 3, 2003) (refusing to shift costs of privilege review of computer hard drives prior to production of hard drive images to requesting party because costs of privilege review for paper documents would not be shifted).

29 Rule 26(b)(2) grants broad discretion to the trial court to guide discovery, and the court is empowered to limit the frequency and/or extent of discovery sua sponte or on motion by a party under Rule 26(c). FED. R. CIV. P 26(b)(2). Rule 26(c) specifies a non-exclusive list of provisions that could be adopted in a protective order, including:

(1) that the disclosure or discovery not be had;
(2) that the disclosure or discovery may be had only on specified terms and conditions, including a designation of the time or place;
(3) that the disclosure or discovery may be had only by a method of discovery other than that selected by the party seeking discovery;
(4) that certain matters not be inquired into, or that the scope of the disclosure or discovery be limited to certain matters;
(5) that discovery be conducted with no one present except persons designated by the court;

***

(7) that a trade secret or other confidential research, development, or commercial information not be revealed or revealed only in a designated way[.]

***

FED. R. CIV. P. 26(c).

producing party seeks a protective order conditioning its production upon payment of costs, including the costs of review. *See* TEX. R. CIV. P. 196.4. Absent proof that the producing party has intentionally deleted information that is relevant to the issues in the case, the protective order should be granted and the requesting party should pay for the costs associated with the request.

14. Sanctions, including spoliation findings, should only be considered by the court if, upon a showing of a clear duty to preserve, the court finds that there was an intentional or reckless failure to preserve and produce relevant electronic data and that there is a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.

Comment 14.a. Knowing, Willful, and Reckless Violations of Preservation Obligations

Due to the complexity of modern computer systems, the large volumes of electronic data, and the continuing changes in information technology, there exists a potential for good faith errors or omissions in the process of preserving and producing electronic information. Neither spoliation findings nor sanctions should issue without proof of a knowing violation of an established duty to preserve or produce electronic data or a reckless disregard for a preservation obligation.[30]

A spoliation finding should require that there be a willful or reckless disregard of an existing discovery order, subpoena, preservation order, or similar preservation obligation. *See New York State Nat'l Org. for Women v. Cuomo*, No. 93 Civ. 7146, 1998 WL 395320, at *2-3 (S.D.N.Y. July 14, 1998) (rejecting sanctions for destroyed computer databases where there was no evidence of bad faith or that plaintiffs were prejudiced by the loss); *see also Stevenson v. Union Pac. R.R. Co.*, ___ F.3d ___, 2003 WL 23104550 at *4-7 (8th Cir. Jan. 5, 2004) (adverse inference instruction (sanction) should not be given on the basis of negligence alone; there must be a finding of bad faith or some other culpable conduct, such as the ongoing destruction of documents during litigation and discovery even after they have been specifically requested). *Cf. Lewy v. Remington Arms Co.*, 836 F.2d 1104, 1112 (8th Cir. 1988) ("[A] court should consider the following factors before deciding whether to give the [spoliation] instruction to the jury. First, the court should determine whether Remington's record retention policy is reasonable considering the facts and circumstances surrounding the relevant documents. Second, in making this determination the court may also consider whether lawsuits concerning the complaint or related complaints have been filed, the frequency of such complaints, and the magnitude of the complaints. Finally, the court should determine whether the document retention policy was instituted in bad faith.").

Ordinarily, the court should not impose sanctions unless the responding party has violated specific restrictions set forth in a court order. *See Kucala Enterprises, Ltd. v. Auto Wax Co.*, No. 02 C 1403, 2003 WL 22433095 (N.D. Ill. Oct. 27, 2003) (adopting Magistrate's recommended dismissal of plaintiff's claim (as well as award of fees and expenses) when plaintiff used "Evidence Eliminator" software to delete information on his computer's hard drive in violation of protective order and after court had granted defendant's motion to compel inspection of the hard drive; district court modified Magistrate's recommended dismissal of non-infringement and allowed defense of counterclaim of infringement in light of the fact that proof for such claims exists outside of evidence deleted but nevertheless conditioned exception

30 This area of law is somewhat unsettled and harmonization of all decisions is difficult. That said, the assessment of sanctions is made along a "continuum of fault—ranging from innocence through the degrees of negligence to intentionality" and counsel should note that certain courts have held that "an adverse inference may be appropriate in some cases involving the negligent destruction of evidence." *See Residential Funding Corp.*, 306 F.3d at 108; see *also* Cmt. 14.b ("Negligent" vs. "Culpable" Spoliation).

on the requirement that plaintiff make all discovery forthwith going forward); *Metro. Opera Ass'n. v. Local 100, Hotel Employees & Rest. Employees Int'l Union,* 212 F.R.D. 178 (S.D.N.Y. 2003) (holding that defendant and its counsel acted willfully and in bad faith in failing to comply with discovery by systematically failing to preserve and produce documents, including disposing of several computers after receiving notice that plaintiff intended to forensically examine those computers, and entering a finding of liability against defendant and awarding attorneys' fees based on discovery abuses). *But see Linnen v. A.H. Robins Co.*, 10 Mass. L. Rptr. 189, No. 97-2307, 1999 WL 462015, at *10 (Mass. Sup. Ct. June 16, 1999) (obligation to cease recycling of backup tapes arose by inference after *ex parte* order governing same was lifted because plaintiff had served broad discovery request on defendant).

Untimely challenges to non-production of information should not, however, provide a basis for a motion for sanctions. *Allen Pen Co. v. Springfield Photo Mount Co.*, 653 F.2d 17, 23 (1st Cir. 1981).

> Illustration i. A party seeks "documents" in discovery and makes no objection to the production of electronic materials without metadata. Shortly before trial, it files a motion for sanctions and an adverse instruction based on the failure to produce metadata. Having not raised the issue earlier, the party has waived the right to seek metadata or sanctions.

Comment 14.b. "Negligent" vs. "Culpable" Spoliation

A number of courts have invoked the tort concept of negligence in addressing spoliation of evidence claims. It is critical, however, to understand that establishing a standard of care (*e.g.*, negligence) does *not* answer the question of whether any sanction is warranted. In particular, the focus should be on culpability: *i.e.*, in the circumstances of the present case, should a party bear culpability (and consequences) for the loss of electronic data? "Culpability" may include what could be considered "negligent conduct," but it does *not* equate all such conduct with an entitlement to sanctions even if the data is lost. For example, failing to take reasonable steps to ensure a good faith effort to preserve relevant electronic data may lead to spoliation instructions or other sanctions. *See Stevenson v. Union Pac. R.R. Co.*, ___ F.3d ___, 2003 WL 23104550, at *4-7 (8th Cir. Jan. 5, 2004) (adverse inference instruction for pre-litigation destruction of evidence through a document retention program cannot be based on negligence alone but requires a finding of bad faith; facts of case supported finding of bad faith pre-litigation destruction of voice tape and the failure to suspend routine destruction of track maintenance records after commencement of suit and receipt of document requests was sanctionable warranting adverse inference instructions, but the absence of evidence of bad faith regarding pre-litigation destruction of track maintenance records rendered inference instruction on loss of those records inappropriate and an abuse of discretion);[31] *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 108 (2nd Cir.

---

31 The *Stevenson* Court explained the distinction between negligent and culpable conduct that would warrant an adverse inference instruction in the circumstances of the case:

> In *Lewy*, we were called upon to address the prelitigation destruction of documents pursuant to a routine document retention policy, but the record was insufficient for us to decide whether the trial court erred by giving the adverse inference instruction. [836 F.2d at 1112] Consequently, we set forth … guidelines for the court to consider on remand, and they include a bad faith consideration. *See id.* By way of example, and as dicta, we also stated that if a corporation "knew or should have known that the documents would become material at some point in the future then such documents should have been preserved." Id. In support of this proposition, however, we quoted *Gumbs v. Int'l Harvester, Inc.*, 718 F.2d 88, 96 (3d Cir. 1983), which states that the adverse inference from the destruction of evidence arises only where the destruction was intentional "and indicates a fraud and a desire to suppress the truth, and it does not arise where the destruction was a matter of routine with no fraudulent intent." Thus, while in dicta we articulated a "knew or should have known" negligence standard, such a standard, standing alone, would be inconsistent with the bad faith consideration and the intentional destruction required to impose an adverse inference for the prelitigation destruction of documents. We have never approved of giving an adverse inference instruction on the basis of prelitigation destruction of evidence through a routine document retention policy on the basis of negligence alone. Where a routine document retention policy has been followed in this context, we now clarify that there must be some indication of an intent to destroy the evidence for the purpose of obstructing or suppressing the truth in order to impose the sanction of an adverse inference instruction. *See Lewy*, 836 F.2d at 1112.

Stevenson v. Union Pac. R.R. Co., 2003 WL 23104550, at *5 (footnote omitted).

2002) (holding that sanctions may be appropriate for negligent failure to take adequate steps to preserve and produce documents in a timely manner); *Wiginton v. CB Richard Ellis, Inc.*, No. 02 C 6832, 2003 WL 22439865, at *7 (N.D. Ill. Oct. 27, 2003) ("[O]nce a party is put on notice that specific relevant documents are scheduled to be destroyed according to a routine document retention policy, and the party does not act to prevent that destruction, at some point it has crossed the line between negligence and bad faith. At that point we must find that the reason for the destruction becomes because the party knew that relevant evidence was contained in the documents and wanted to hide the adverse information, rather than because the documents were scheduled to be destroyed.").[32] If a party has specifically requested documents in electronic format, allowing those documents to be destroyed, even if hard copies of those documents still exist, can lead to sanctions. *See Lombardo v. Broadway Stores, Inc.,* 2002 WL 86810, at *8 (Cal. App. Jan. 22, 2002) (affirming sanctions award for allowing and concealing loss of electronic files and rejecting the argument that there was no spoliation when paper copies of the documents still existed).

Comment 14.c. Prejudice

A party seeking sanctions should be required to prove that there is a reasonable likelihood the party has been materially prejudiced by the act complained of. *See, e.g., Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243, 2003 WL 22410619, at *6 (S.D.N.Y. Oct. 22, 2003) ("In order to receive an adverse inference instruction, Zubulake must demonstrate not only that UBS destroyed relevant evidence as that term is ordinarily understood, but also that the destroyed evidence would have been favorable to her."); *Concord Boat Corp. v. Brunswick Corp.,* No. LR-C-95-781, 1997 WL 33352759, at *7 (E.D. Ark. Aug. 29, 1997) (holding that destruction of "tangentially relevant" e-mail would not justify imposition of sanctions); *Allen Pen Co. v. Springfield Photo Mount Co.*, 653 F.2d 17, 24 (1st Cir. 1981) (destruction of evidence that could be obtained from other sources does not support adverse inference sanction); *cf. Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 112-13 (2nd Cir. 2002) (court held that, absent a showing of prejudice, the jury's verdict in favor of the producing party should not be disturbed on remand but that court could nevertheless consider discovery sanctions if it found that the producing party acted "with a culpable state of mind").

An award of sanctions without a showing of prejudice is particularly inappropriate in the context of electronic discovery, which often involves searching through many thousands or even many millions of files and messages. Given the volumes of data involved, such processes are bound to be imperfect, and data can be inadvertently missed in the discovery process.

If a party believes it may be sanctioned for failing to produce data, even when the failure did not prejudice the opponent, producing parties will have incentives to produce a vastly over-inclusive set of data to guarantee that every conceivably relevant item is included. Such a result would impose unnecessary costs on both the requesting party and the producing party. Neither the letter nor the spirit of the discovery rules requires this approach.

Comment 14.d. The Good Faith Destruction of Documents in Compliance with a Reasonable Records Management Policy Should Not be Considered Sanctionable Conduct Absent Reasonable Notice to the Organization of a Duty to Preserve the Documents.

32 In *Wiginton*, the court noted that the defendant could have taken steps to search for electronic documents but did not and concluded that the "complete failure to perform any search rises above the level of mere negligence, and this willful blindness in the context of the facts surrounding the destruction of the documents, leads us to find that the documents were destroyed in bad faith." *Wiginton v. CB Richard Ellis, Inc.*, No. 02 C 6832, 2003 WL 22439865, at *7 (N.D. Ill. Oct. 27, 2003) (court also noted that "bad faith" was not a precondition to the imposition of sanctions).

Where a party destroys documents in good faith under a reasonable records management policy, no sanctions should attach. Of course, this does not mean a party with a records management policy may destroy documents with impunity as long as that destruction has a basis in the policy. To the contrary, "[t]he duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation." *Silvestri v. General Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001). Once an organization reasonably anticipates that documents in its possession may be relevant to reasonably foreseeable litigation, the organization should preserve those documents, even if a records management program calls for the routine destruction of those documents. As one court recently noted, this requires answering two separate questions: "*when* does the duty to preserve attach, and *what* evidence must be preserved." *Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243, 2003 WL 22410619, at *2 (S.D.N.Y. Oct. 22, 2003).

Failure to properly preserve documents may result in sanctions, including monetary fines, instructions to the jury commanding them to infer that the destroyed documents would be adverse to the interests of the responding party, and, in extreme cases, default judgments. *See, e.g., Carlucci v. Piper Aircraft Corp.*, 102 F.R.D. 472 (S.D. Fla. 1984) ("Having determined that Piper intentionally destroyed documents to prevent their production, the entry of a default is the appropriate sanction."). Therefore, an organization's records management policy should recognize that the organization will sometimes have to suspend its ordinary retention and disposition of records, and should include procedures designed to implement such suspensions.

However, if a party does not reasonably anticipate litigation, the destruction of documents in compliance with a reasonable records management policy should not be considered sanctionable conduct. Instead, the fact that the destruction occurred in compliance with a preexisting policy should be considered *prima facie* evidence of the good faith of the organization. Thus, for example, in *Vick v. Texas Employment Commission*, the plaintiff alleged that there should be an adverse inference against the defendant for the improper destruction of records. 514 F.2d 734 (5th Cir. 1975). The court denied the claim, holding that:

> [The] records on Vick were destroyed before trial, apparently pursuant to Commission regulations governing disposal of inactive records. Vick's argument is unpersuasive. The adverse inference to be drawn from destruction of records is predicated on bad conduct of the defendant … There was indication here that the records were destroyed under routine procedures without bad faith and well in advance of Vick's service of interrogatories. Certainly, there were sufficient grounds for the trial court to so conclude.

Id. at 737. As one commentator has noted, "in the absence of a duty to preserve records, courts have consistently refused to sanction parties who have destroyed records pursuant to a records retention program." Donald S. Skupsky and John C. Montaña, Law, Records and Information Management at 134 (1994).[33]

33 It should be noted that even in a circumstance where an adverse inference instruction (sanction) may be appropriate, the party should be allowed an opportunity "to put on some evidence of its document retention policy and how it affected the destruction of the requested records as an innocent explanation for its conduct." *Stevenson v. Union Pac. R.R. Co.*, ___ F.3d ____, 2003 WL 23104550 at *7 (district court abused its discretion by not allowing reasonable rebuttal to inference; "[a]bsent this opportunity, the jury is deprived of sufficient information on which to base a rational decision of whether to apply the adverse inference, or an otherwise permissive inference easily becomes an irrebuttable presumption.").

APPENDIX A: GLOSSARY

Active Data: Active Data is information residing on the direct access storage media of computer systems, which is readily visible to the operating system and/or application software with which it was created and immediately accessible to users without undeletion, modification or reconstruction.

Archival Data: Archival Data is information that is not directly accessible to the user of a computer system but that the organization maintains for long-term storage and record keeping purposes. Archival data may be written to removable media such as a CD, magneto-optical media, tape or other electronic storage device, or may be maintained on system hard drives in compressed formats.

Backup Data: Backup Data is information that is not presently in use by an organization and is routinely stored separately upon portable media, to free up space and permit data recovery in the event of disaster.

Backup Tape: *See* Disaster Recovery Tape.

Backup Tape Recycling: Backup Tape Recycling describes the process whereby an organization's backup tapes are overwritten with new backup data, usually on a fixed schedule (*e.g.*, the use of nightly backup tapes for each day of the week with the daily backup tape for a particular day being overwritten on the same day the following week; weekly and monthly backups being stored offsite for a specified period of time before being placed back in the rotation).

Computer Forensics: Computer Forensics is the use of specialized techniques for recovery, authentication, and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel.

Data Mining: "Data Mining" generally refers to techniques for extracting summaries and reports from an organization's databases and data sets. In the context of electronic discovery, this term often refers to the processes used to cull through a collection of electronic data to extract evidence for production or presentation in an investigation or in litigation. Data mining can also play an important role in complying with data retention obligations under an organization's formal document management policies.

De-Duplication: De-Duplication ("De-Duping") is the process of comparing electronic records based on their characteristics and removing duplicate records from the data set.

Deleted Data: Deleted Data is data that, in the past, existed on the computer as live data and which has been deleted by the computer system or end-user activity. Deleted data remains on storage media in whole or in part until it is overwritten by ongoing usage or "wiped" with a software program specifically designed to remove deleted data. Even after the data itself has been wiped, directory entries, pointers, or other metadata relating to the deleted data may remain on the computer.

Deletion: Deletion is the process whereby data is removed from active files and other data storage structures on computers and rendered inaccessible except using special data recovery

tools designed to recover deleted data. Deletion occurs in several levels on modern computer systems: (a) File level deletion: Deletion on the file level renders the file inaccessible to the operating system and normal application programs and marks the space occupied by the file's directory entry and contents as free space, available to reuse for data storage. (b) Record level deletion: Deletion on the record level occurs when a data structure, like a database table, contains multiple records; deletion at this level renders the record inaccessible to the database management system (DBMS) and usually marks the space occupied by the record as available for reuse by the DBMS, although in some cases the space is never reused until the database is compacted. Record level deletion is also characteristic of many e-mail systems. (c) Byte level deletion: Deletion at the byte level occurs when text or other information is deleted from the file content (such as the deletion of text from a word processing file); such deletion may render the deleted data inaccessible to the application intended to be used in processing the file, but may not actually remove the data from the file's content until a process such as compaction or rewriting of the file causes the deleted data to be overwritten.

Disaster Recovery Tape: Disaster Recovery Tapes are portable media used to store data that is not presently in use by an organization to free up space but still allow for disaster recovery. May also be called "Backup Tapes."

Distributed Data: Distributed Data is that information belonging to an organization which resides on portable media and non-local devices such as home computers, laptop computers, floppy disks, CD-ROMs, personal digital assistants ("PDAs"), wireless communication devices (*e.g.*, Blackberry), zip drives, Internet repositories such as e-mail hosted by Internet service providers or portals, web pages, and the like. Distributed data also includes data held by third parties such as application service providers and business partners.

Document: *See* Rule 34 of the Federal Rules.

Electronic Mail: Electronic Mail, commonly referred to as e-mail, is an electronic means for communicating information under specified conditions, generally in the form of text messages, through systems that will send, store, process, and receive information and in which messages are held in storage until the addressee accesses them.

Forensic Copy: A Forensic Copy is an exact bit-by-bit copy of the entire physical hard drive of a computer system, including slack and unallocated space.

Fragmented Data: Fragmented data is live data that has been broken up and stored in various locations on a single hard drive or disk.

Instant Messaging ("IM"): Instant Messaging is a form of electronic communication which involves immediate correspondence between two or more users who are all online simultaneously.

Legacy Data: Legacy Data is information in the development of which an organization may have invested significant resources and which has retained its importance, but which has been created or stored by the use of software and/or hardware that has been rendered outmoded or obsolete.

Metadata: Metadata is information about a particular data set which may describe, for example, how, when, and by whom it was received, created, accessed, and/or modified and how it is formatted. Some metadata, such as file dates and sizes, can easily be seen by users;

other metadata can be hidden or embedded and unavailable to computer users who are not technically adept. Metadata is generally not reproduced in full form when a document is printed. (Typically referred to by the less informative shorthand phrase "data about data," it describes the content, quality, condition, history, and other characteristics of the data.)

Migrated Data: Migrated Data is information that has been moved from one database or format to another, usually as a result of a change from one hardware or software technology to another.

Pointer: A pointer is an index entry in the directory of a disk (or other storage medium) that identifies the space on the disc in which an electronic document or piece of electronic data resides, thereby preventing that space from being overwritten by other data. In most cases, when an electronic document is "deleted," the pointer is deleted, which allows the document to be overwritten, but the document is not actually erased.

Residual Data: Residual Data (sometimes referred to as "Ambient Data") refers to data that is not active on a computer system. Residual data includes (1) data found on media free space; (2) data found in file slack space; and (3) data within files that has functionally been deleted in that it is not visible using the application with which the file was created, without use of undelete or special data recovery techniques.

Sampling: Sampling usually (but not always) refers to the process of statistically testing a data set for the likelihood of relevant information. It can be a useful technique in addressing a number of issues relating to litigation, including decisions as to which repositories of data should be preserved and reviewed in a particular litigation, and determinations of the validity and effectiveness of searches or other data extraction procedures. Sampling can be useful in providing information to the court about the relative cost burden versus benefit of requiring a party to review certain electronic records.

APPENDIX B: AUTHORITIES CITED

Federal Cases

State Cases

Statutes and Regulations

Rules

Other Authorities

Miscellaneous

APPENDIX C:

SUGGESTED CITATION FORMAT
REQUESTS FOR REPRINT PERMISSION

Suggested Citation Format:

This publication may be cited as follows:

The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery (Sedona Conference℠ Working Group Series 2004).

The recommended short citation form is simply:

The Sedona Principles (2004), 5 Sedona Conf. J at p. 151 et.seq. (2004).

It may be appropriate to cite specific pages, principles, or comments. For example:

The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery 3-4 (Sedona Conference Working Group Series 2004).

The Sedona Principles, Principle 11.

The Sedona Principles, Cmt. 5.e.

The Sedona Principles, 5 Sedona Conf. J. 151, p__ (2004).

Requests for Reprint Permission:

APPENDIX D*:
2003-04 WORKING GROUP PARTICIPANTS, MEMBERS & OBSERVERS

Sharon A. Alexander, Esquire
Jones Day
Participant 1 2

Jacqueline M. Algon, Ph.D.
Merck & Co., Inc.
Participant 2

Thomas Y. Allman, Esquire
BASF Corporation
Participant; Steering Committee 1 2

Thomas Barnett, Esquire
Electronic Evidence Discovery, Inc.
Participant 1

Jason R. Baron, Esquire
National Archives and Records Administration
Observer 2

Charles A. Beach, Esquire
Exxon Mobil Corporation
Participant 2

Steven C. Bennett, Esquire
Jones Day
Participant 1 2

The Hon. Richard E. Best (Ret.)
Action Dispute Resolution Services
Observer 2

Alan F. Blakley, Esquire
Blakley Law Office
Member

Richard G. Braman, Esquire
The Sedona Conference
Gray Plant Mooty
Observer; Executive Director 1 2

Hildy Bowbeer, Esquire
3M
Member

Christine M. Burns
Cohasset Associates, Inc.
Participant 2

Harold Callet
Oracle
Member

The Honorable John L. Carroll (Ret.)
Cumberland School of Law
Samford University
Observer 1 2

Barbara Caulfield, Esquire
Affymetrix, Inc.
Member

R. Noel Clinard, Esquire
Hunton & Williams
Participant 1 2

Connor R. Crowley, Esquire
Finkelstein, Thompson & Loughran
Member 2

M. James Daley, Esquire
Shook, Hardy & Bacon LLP
Participant 1 2

David E. Dukes, Esquire
Nelson, Mullins, Riley & Scarborough, LLP
Participant 1

Robert A. Eisenberg, Esquire
CoreFacts
Participant 1 2

Laura E. Ellsworth, Esquire
Jones Day
Participant 2

Amor A. Esteban, Esquire
Drinker Biddle & Reath LLP
Participant 2

Jason B. Fliegel, Esquire
Mayer, Brown, Rowe & Maw LLP
Participant; Senior Editor

Peter Freeman, Esquire
Ernst & Young
Participant 2

Sherry Harris
Hunton & Williams
Participant 1 2

Ted S. Hiser, Esquire
Jones Day
Participant; Senior Editor Y F

Editor's Note: *This list represents the Working Group composition as of October, 2003. The Group has substantially expanded since that time, and some associations have changed. *See also* Note at the end of this Appendix.

Geoffrey M. Howard
Bingham McCutchen LLP
Member

David A. Irvin, Esquire
Womble Carlyle Sandridge & Rice
Participant 1 2

Conrad Jacoby, Esquire
Potomac Consulting Group
Participant

John H. Jessen
Electronic Evidence Discovery, Inc.
Participant; Steering Committee 1 2
Technology Advisor

Larry G. Johnson, Esquire
Legal Technology Group, Inc.
Participant

Jeffrey J. Joyce, Esquire
Jones Day
Participant 2

Sidney Kanazawa, Esquire
Van Etten Suzumoto & Becket, LLP
Participant 1

David Kittrell
Participant 2

Monica Latin, Esquire
Carrington Coleman
Member

R. Michael Leonard, Esquire
Womble Carlyle Sandridge & Rice
Participant 1

John P. Mancini, Esquire
LeBoeuf, Lamb, Greene & MacRae L.L.P.
Participant 2

Wayne Matus, Esquire
LeBoeuf, Lamb, Greene & MacRae L.L.P.
Member

J.J. McCracken, Esquire
Cooper Tire & Rubber Company
Participant 1 2

James L. Michalowicz
DuPont
Participant 1 2

Bruce Miller
IBM Canada Ltd.
Member

Denise M. Mineck, Esquire
Life Investors Insurance Company
of America
Member

Timothy L. Moorehead, Esquire
BP America, Inc.
Participant; Steering Committee 1 2

Kate Oberlies O'Leary, Esquire
General Electric Company
Participant 2

Timothy M. Opsitnick, Esquire
JurInnov Ltd.
Participant 1 2

Laura Lewis Owens, Esquire
Alston & Bird, LLP
Participant 2

Robert W. Pass, Esquire
Carlton Fields
Participant 2

Richard Pearce-Moses
Arizona State Library, Archives
and Public Records
Observer 2

Vivian Polak, Esquire
LeBoeuf, Lamb, Greene & MacRae L.L.P.
Member

Ashish S. Prasad, Esquire
Mayer, Brown, Rowe & Maw LLP
Participant; Executive Editor 1 2

Michael J. Prounis
Evidence Exchange
Participant 2

Charles R. Ragan, Esquire
Pillsbury Winthrop LLP
Participant 1 2

Jonathan M. Redgrave, Esquire
Jones Day
Participant; Steering Committee (Chair) 1 2
Editor-in-Chief

Dan Regard, Esquire
FTI Consulting, Inc.
Participant 1 2

Mark V. Reichenbach
Pillsbury Winthrop LLP
Participant 1 2

Paul M. Robertson, Esquire
Bingham McCutchen LLP
Participant 1 2

Herbert L. Roitblat, Ph.D.
DolphinSearch, Inc.
Participant 2

Andrea D. Rose, Esquire
Crowell & Moring, LLP
Member

John J. Rosenthal, Esquire
Howrey Simon Arnold & White
Participant 2

Leigh R. Schachter, Esquire
Verizon Wireless
Participant 1

Gregory P. Schaffer, Esquire
PriceWaterhouseCoopers LLP
Participant 2

The Hon. Shira A. Scheindlin
United States District Court for the
Southern District of New York
Observer 2

Kenneth Shear, Esquire
Electronic Evidence Discovery, Inc.
Participant 1 2

Peter B. Sloan, Esquire
Blackwell Sanders Peper Martin, LLP
Member

George J. Socha, Jr., Esquire
Socha Consulting LLC
Participant 2

Judy Van Dusen
VanKorn Group, Limited
Participant 2

Lori Ann Wagner, Esquire
Faegre & Benson LLP
Participant 1 2

Megan A. Walker
Ford Motor Company
Participant 1

Robert F. Williams
Cohasset Associates, Inc.
Participant 1 2

Scott L. Winkelman, Esquire
Crowell & Moring LLP
Member

Kenneth J. Withers, Esquire
Federal Judicial
Center
Observer 1 2

Edward C. Wolfe, Esquire
General Motors Corp.
Participant 2

John W. Woods, Esquire
Hunton & Williams
Member

Susan B. Wortzman, Esquire
Lerners LLP
Participant 2

[This list is current as of the second annual meeting of the Working Group, in October of 2003. As with all our active Working Groups, membership is open and ongoing. See The "Working Group Series" Section on our website: www.thesedonaconference.org for further details on our Working Group Membership Program.]

1 = Attended October 2002 Annual WG Meeting
2 = Attended October 2003 Annual WG Meeting

APPENDIX E:
BACKGROUND ON THE SEDONA CONFERENCE℠ & ITS WORKING GROUP SERIES

The Sedona Conference℠ is a nonprofit, 501(c)(3) research and education institute dedicated to the advancement of law and policy in the areas of antitrust, complex litigation and intellectual property rights. The Sedona Conference℠ meets that goal in part through the stimulation of ongoing dialogues among leaders of the bench and bar in each area under study. To that end, The Sedona Conference℠ hosts three major conferences each year in unique, retreat-like settings. Fifteen of the nation's finest jurists, attorneys, academicians and others prepare written materials for, and lead the discussions during, each two-day conference.

What sets our conferences apart from all other legal study programs is the quality and intensity of the dialogues, generating cutting-edge analyses. To ensure the proper environment for this level of interaction, each conference is strictly limited to 45 experienced participants in addition to the faculty (who remain and participate throughout the entire conference). The best of the written materials are then published annually in *The Sedona Conference Journal,* which is distributed on a complimentary basis to courthouses and public law libraries around the country and by subscription to others. The Journal is also available on Westlaw and is listed in H.W. Wilson's Index to Legal Periodicals. The Sedona Conference℠ has received broad and strong accolades from participants since its inception. (See "Raves" section of our website).

The Sedona Conference℠ Working Group Series is designed as a bridge between our advanced legal conferences and an open think-tank model that can produce authoritative works designed to stimulate the development of the law. Working Groups in the Series begin with the same high caliber of participants as our regular season conference faculty and participants. The total "active" Group, however, is limited to less then 40 (though anyone can join The Working Group Membership Program to gain access to an individual Working Group's work area). The Group circulates ideas, questions, developments and references ahead of a face-to-face meeting. At the meeting, decisions are made regarding the form, direction and content of the output, teams are assembled, and the drafting gets underway. Following a few months of work, a public comment version is then published and subjected to peer review before the "final" work product is published. Consistent with our mission, all "public comment" drafts and completed Working Group publications are available for free dowload for individual use from our website. For details on reprint permission, see the "publications" area of our website or contact us at tsc@sedona.net.

Funding for The Sedona Conference℠ comes from individuals, law firms and corporations, in the form of conference sponsorships and registration fees. Funding for the 2003-04 Working Group Addressing Electronic Document Retention and Production came from individual Working Group membership fees, as well as sponsorships provided by Electronic Evidence Discovery, Inc., Jones Day, Mayer Brown Rowe & Maw LLP (Founding Sponsors), and Carrington Coleman Sloman & Blumenthal, Ernst & Young, and PricewaterhouseCoopers (Supporting Sponsors).

If you are interested in contributing to the efforts of The Sedona Conference℠ or any of its Working Groups, sponsorship opportunities, or if you want more information about The Sedona Conference℠, generally, you can visit www.thesedonaconference.org or contact the Executive Director, Richard G. Braman, at the following address:

The Sedona Conference
180 Broken Arrow Way South
Sedona, Arizona 86351

Voice: 1.866.860.6600 Toll Free or 1.928.284.2698
Facsimile: 1.928.284.4240
E-mail: tsc@sedona.net