IMPORTANT NOTICE:
This Publication Has Been Superseded

See the Most Current Publication at

https://thesedonaconference.org/publication/The_Sedona_Principles

wgs℠

THE SEDONA PRINCIPLES:

Best Practices Recommendations & Principles for Addressing Electronic Document Production

A Project of the October 2002
Sedona Conference Working Group on
Best Practices for Electronic Document
Retention & Production

March 2003

The Sedona Conference℠

The Sedona Principles

Editor-in-Chief: Jonathan M. Redgrave, Esq.
Senior Editor: Ashish Prasad, Esq.
Editors: Jason Fliegel, Esq.
Ted S. Hiser, Esq.

wgs℠

Visit www.thesedonaconference.org

Foreword

Welcome to the first publication in The Sedona Conference[SM] Working Group Series (the "WGS"). The WGS[SM] is designed to bring together some of the nation's finest lawyers, consultants, academics and jurists to address current problems in the areas of antitrust law, complex litigation and intellectual property rights that are either ripe for solution or in need of a "boost" to advance law and policy. (*See* Appendix C for further information about The Sedona Conference[SM] in general, and the WGS[SM] in particular). The WGS[SM] output is published and widely distributed for review, critique and comment. Following a period of peer review, we will revise and republish the original piece, taking into consideration what has been learned during the comment period. The Sedona Conference[SM] hopes and anticipates that the output of its working groups will evolve into authoritative statements of law and policy, both as they are and as they ought to be.

Electronic document production is an ideal first topic for the WGS[SM]. The problems posed vex corporations, litigants, and the courts alike, yet there exist few guides sufficient to meet the complexity of issues that even the most simple document request can raise. The Steering Committee and participants of the Working Group on Electronic Document Production are to be congratulated for their efforts developing these guidelines and their continued dedication to the project since the first meeting in October of 2002. I especially want to acknowledge the contributions of Jonathan Redgrave in organizing and leading the Working Group. Special thanks also to Electronic Evidence Discovery, Inc. for sponsoring the effort. Finally, the peer review period is an important part of the balanced development of these principles and commentary; please submit your comments in writing to Jonathan (jredgrave@jonesday.com) and me (tsc@sedona.net) on or before June 1, 2003. Thank you in advance for any thoughts you may take the time to forward to us as this dynamic document takes shape.

Richard G. Braman
Executive Director
The Sedona Conference[SM]

Table of Contents

Introduction

In Spring 2002, many of us who would later form the Sedona Conference Working Group on Electronic Document Production began to discuss ways to develop "best practices" for lawyers to follow in addressing electronic document production. An industry of electronic discovery consultants and continuing legal education courses had developed, which suggested to some that all data ever generated electronically would be saved and made available for litigation. Courts handled ripe disputes, but with few decisions reported and a smaller number containing applicable guidance outside the context of the instant facts, organizations were uncertain as to their legal obligations. The collapse of Enron and Arthur Andersen, and the legislative response to these events, including the Sarbanes-Oxley Act of 2002, confirmed the importance of handling electronic document production in a defensible manner. It seemed doubtful to us that the normal development of case law would yield, in a timely manner, best practices for organizations to follow in the production of electronic documents.

In October 2002, The Sedona Conference Working Group on Electronic Document Production, a group of attorneys and consultants experienced in electronic discovery matters, met to address the production of electronic data and documents in discovery. The group was concerned about the adequacy of rules and concepts that were developed largely for paper discovery to handle issues of electronic discovery. After vigorous debate, key principles emerged for addressing electronic data and document production. This document contains those principles, and the reasons supporting them.

In thinking about electronic document production, one might begin by looking at the Federal Rules of Civil Procedure. Under Rule 34 and many of its state counterparts, all "data compilations" are documents and therefore might be handled with procedures and methodologies created for paper documents. However, it is important to recognize the significant differences between paper and electronic information in terms of structure, content and volume. Simply put, the way in which information is created, stored and managed in digital environments is inherently and fundamentally different from the way in which that is done in the paper world. For example, the simple act of typing a letter on a computer involves multiple (and ever changing) hidden steps, databases, tags, codes, loops, and algorithms that simply have no paper analogue. The interpretation and application of the discovery rules, to date, has not accommodated these differences consistently and predictably so that litigants can efficiently and cost effectively meet discovery obligations without risk of unforeseeable sanctions.

The Sedona Conference Working Group on Electronic Document Production was conceived as an effort to develop reasonable principles to guide organizational practices and legal doctrine. The participants were chosen based on their knowledge and practical experience with electronic discovery issues. The group welcomes the comments of bench and bar alike on the principles, which we hope will guide lawyers and judges who are confronted with electronic document production issues in the coming years.

In drafting the principles and commentary, we tried to keep in mind the "rule of reasonableness." That rule, embodied in Rules 1 (courts should secure the just, speedy and inexpensive determination of all matters) and 26(b)(2) (proportionality test of burden, cost and need) of the Federal Rules of Civil Procedure, and in many of their state counterparts, stands for the basic proposition that courts and litigants must permit that discovery that is reasonable and appropriate to the dispute at hand.

We believe that this "rule of reasonableness" analysis is a useful guide in discussions of electronic document production, including, for example, the question of whether computer forensics should be used to unearth "hidden" data.

This paper has three major sections. The first outlines why courts and litigants need reasonable standards to address electronic data and document production. Some have suggested that our current laws and rules are sufficient to meet the needs of electronic issues; this section outlines why those laws and rules are not sufficient. The second section sets forth basic principles of electronic document production. These principles embody the consensus views of the Working Group participants, and represent a reasonable and balanced approach to the treatment of electronic data. The third section contains commentary on those principles, and aims to expand the basic formulations set forth in the principles into a more comprehensive analysis.

Our earnest hope is that the efforts of the Working Group will stimulate productive discussion and promote the formulation of legal doctrine consistent with principles of fairness, equity and efficiency.

Thomas Y. Allman
Gary L. Hayden
John H. Jessen
Timothy L. Moorehead
Jonathan M. Redgrave[1]

March 15, 2003

[1] Readers should note that this effort represents the collective view of The Sedona Conference Working Group on Electronic Document Production and does not necessarily reflect or represent the views of The Sedona Conference[SM], any one participant (or observer) or law firm/company employing a participant or any of their clients. A list of all participants (as well as observers to the process) is set forth in Appendix B.

The Need For Reasonable Standards To Address Electronic Data And Documents In Discovery

Before turning to the principles that the Working Group developed to address electronic document production, it is first necessary to discuss whether such standards are necessary in the first place. In short: Do courts, parties and counsel need any specific guidance in the area? The Working Group concluded that the answer to this question is "yes." This section sets forth the rationale behind that answer.

1. Electronic Documents Are Different Than Paper Documents

Since 1970, the definition of a "document" in Rule 34 of the Federal Rules of Civil Procedure has included a reference to electronic data.[2] The role of electronic evidence in discovery is well recognized, as reflected in an oft-quoted passage from Wright & Miller:

> [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.'[3]

However, this principle – that storing information in an electronic format does not exclude it from the realm of potential discovery — does not provide specific guidance on where courts and litigants should draw the lines in applying the proportionality test of Rule 26 to electronic discovery requests and disputes. In order to draw those lines, one needs to understand the differences between electronic documents and paper documents. The distinctive characteristics of electronic documents can be divided into quantitative and qualitative differences between electronic and paper documents.

A. Quantitative Differences

There are several quantitative differences between electronic and paper documents. First, 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 — 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, or

---

2 The Advisory Committee Notes for the 1970 amendments to the Federal Rules of Civil Procedure reflect the inclusive nature of the term "document":

> The inclusive description of "documents" is revised to accord with changing technology. It makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when the 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. [emphasis supplied].

3 8A Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice & Procedure,* § 2218 at 449 (2d ed. 1994) (quoting *Bills v. Kennecott Corp.,* 108 F.R.D. 459, 462 (D. Utah 1985)) (emphasis added). 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), § 21.446 (1995).*

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,[4] 70 percent of corporate records may be stored in electronic format,[5] and 30 percent of electronic information is never printed to paper.[6] 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 millions of printed pages. Organizations often accumulate thousands of such tapes as data is stored, transmitted, copied, replicated, backed up, and archived.

Second, the frequent obsolescence of numerous computer systems due to changing technology creates unique issues for recovering electronic documents that are not present in 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 archival systems nor the technological infrastructure necessary to restore the out-of-date systems may be available when it comes time to access this "legacy" data. In a perfect world, electronic records that continue to be needed 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.

Third, electronic documents are more easily replicated than paper documents. While paper documents can be copied, 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 communication 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 this 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.[7]

Fourth, electronic documents are more difficult to dispose of than paper documents. A shredded paper document is, for all intents and purposes, irretrievable. Likewise, a paper document that has been discarded and taken off the premises is generally considered to be beyond recovery. When a computer user deletes an electronic file, the computer simply removes a pointer to the body of the electronic data in a directory — it does not delete the body of the document itself. Only when the computer requires the space that the particular file occupies will the content be partially or completely overwritten. As a result, computer systems may retain documents long after their users believe those documents are gone.

---

[4] Kenneth J. Withers, *The Real Cost of Virtual Discovery,* Federal Discovery News (Feb. 2001) .

[5] Lori Enos, *Digital Data Changing Legal Landscape,* E-Commerce Times, May 16, 2000.

[6] Richard L. Marcus, *Confronting the Future: Coping with Discovery of Electronic Materials,* 64 Sum Law & Contemp. Probs. 253, 280-81 (2001).

[7] 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 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.

This fact compounds the rate at which electronic data and documents accumulate and creates an entire subset of electronic data that exist unknown to the individuals with ostensible custody over them. Indeed, in recognition of the lack of effectiveness of simply deleting electronic documents, software is sold that purports to actually erase or wipe the data by overwriting the data numerous times.

B. Qualitative Differences

There are also several qualitative differences between electronic and paper documents. First, computer information, unlike paper, has dynamic content that is designed to change over time even without human intervention. Examples include the following: 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 being 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.

Second, electronic data, unlike paper, may be incomprehensible when separated from their environments. For example, as a structured set of data, the information in a database is generally 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. In order to make sense of the data, a viewer needs the context that includes labels, columns, report formats and other information.[8] Often this can take the form of existing or customized "reports" that can be generated, obviating any need to access or produce the underlying database.

Third, 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 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.

Fourth, electronic documents, unlike paper, contain metadata, information used by the computer to manage and often classify the document that is not visible to the user. The ability to process and manipulate electronic data is facilitated by formatting codes and other information that are part of the document or file yet are not visible to the user. There are many examples of metadata.[9]

---

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

[9] Such information includes file designation, create and edit dates, authorship, comments, and edit history. Indeed, electronic files contain hundreds or even thousands of pieces of such information distinct from the user created content of a file. E-mail has its own metadata elements that include, among about 800 or more properties, such information as dates that mail was sent, received, replied to or forwarded, blind carbon copy ("bcc") information, and sender address book information. 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 allows 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.

Fifth, it is more difficult to determine the provenance of electronic documents than paper documents. It is generally a routine matter to determine the authorship, or at least the custodianship, of a written document. Factors such as handwriting, signatures, and the location of the document facilitate such determinations. The manner in which electronic data is created, stored and transmitted makes determination of authorship a greater challenge. Electronic files are often stored in shared network folders that may have departmental or functional designations rather than author information. In addition, there is greater use of collaborative software that allows for group creation of electronic data, rendering the determination of authorship far more difficult. The ease of transmitting electronic data and the routine modification and multi-user editing process that often takes place further complicate the issue. Finally, while electronic documents may be stored on an individual's hard drive, it is likely that such documents may 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.

In real 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 reports. In the electronic age, such a command could present intractable problems. Because electronic information is both dynamic (*i.e.,* constantly changing) and ubiquitous, short of suspending operations, all electronic data, wherever located and in whatever form, will have to be copied so that reports can be generated as needed in the future. 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]

2. Standards For Dealing With Electronic Data And Documents Are Necessary And Appropriate

There are standards that govern the scope of discovery regardless of the resources available, the matters at issue, or whether a party is a defendant or plaintiff. For example, under the Federal Rules of Civil Procedure, depositions presumptively are limited to one day of seven hours. *See* Fed. R. Civ. P. 30(d)(2). Interrogatories presumptively are limited to 25 in number. *See* Fed. R. Civ. P. 33(a). All discovery is subject to the limitations of Rule 26. *See* Fed. R. Civ. P. 26(a)(1)(B) (disclosure of documents and things limited to those "in the possession, custody or control of the party and that the disclosing party may use to support its claims or defenses…"); Fed. R. Civ. P. 26(b)(1) (party may obtain discovery "regarding any matter, not privileged, that is relevant to the claim or defense of any party …").

Rule 26(b)(2)(i) further 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." Rule 26(b)(2)(iii) provides a standard for limiting discovery, *i.e.,* if "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 dispute." Local court rules likewise contain many rules or standards imposing limitations on all forms of discovery. These existing rules, however, do not account for the dramatic and substantial differences between electronic and paper documents outlined above. For example, an inartfully worded preservation order applied to electronic

[10] Indeed, at an extreme such data might be interpreted to include machine or product line data that is collected for milliseconds, and attempting to retain all such data would effectively shut down manufacturing operations as retaining all data would quickly outstrip the storage capacity.

records could cause a litigant to incur costs that are multiples of the value of the case before discovery even begins. Simply put, as a result of the qualitative and quantitative differences between electronic and paper documents, the current rules do not effectively address a myriad of issues unique to electronic documents.

Some have argued that there is no need for electronic document production standards because the Federal Rules of Civil Procedure provide an adequate framework to address issues that arise. The Working Group rejected this argument for several reasons. First, we have 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 sought by the opposing party later in discovery.

Second, we believe that the unfair burdens would be minimized if standards were provided to parties and courts for addressing electronic document production. In the absence of 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 of Civil Procedure 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,* 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 Fed. R. Civ. P. 34 Up to the Task?,* 41 B.C. L. Rev. 327, 361 (2000) ("[W]hile courts have managed to resolve motions that raise Fed. R. Civ. P. 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]

We believe that electronic document production standards arising out of our practical experiences would bring needed predictability to litigants and guidance to courts. The principles set forth herein are concrete enough to provide actual direction, but flexible enough to allow courts within their sound discretion to fashion solutions for the inevitable exceptions. For example, while documents and data in a computer or electronic device may be discoverable under Fed. R. Civ. P. 34 or its state law equivalents, we argue that discovery of all such documents and data is simply not feasible. Because the volume of

[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.,* 1999 Mass. Super. LEXIS 240 (Mass. Super Ct. June 15, 1999) (obligation imposed to cease recycling of backup tapes); *compare, e.g., In re Brand Name Prescription Drugs Antitrust Litig.,* (1995 WL 360526 at *3) (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 (S.D.N.Y. Jan. 16, 2002) (adopting multiple factor test to address cost allocation of electronic discovery burden).

such information captured in computer systems today is already enormous, and increasing exponentially, the discovery of electronic data and documents must be firmly grounded in the principles of promoting the just, speedy, and inexpensive resolution of civil disputes and making the burden of discovery proportional to the anticipated benefit, consistent with Fed. R. Civ. P. 1 and 26 and their state law analogues.

To serve this end, *dialogue and reasonableness are essential.* Parties are well served by an early discussion about the issues in dispute, the types of information sought, the likely databases where such information may be stored, and the realistic costs of preserving, retrieving, producing, and reviewing such data. Electronic discovery is a tool to help resolve a dispute and should not be viewed as a strategic weapon to coerce unjust, delayed, or expensive results. The need for good faith of the parties also extends to the efforts taken to reasonably retain relevant electronic data, the form of the production, and the allocation of the costs of the preservation and production. Each of these aspects of discovery should be considered in light of the nature of the litigation and amount in controversy, as well as the cost, burden and disruption to parties' operations.[12]

[12] As a practical matter, such disputes are most likely to arise and require court intervention when the burdens of preservation and production are disproportionate among the litigants such as, for example, in products liability lawsuits brought by individuals with few, if any, electronic records, against large corporations with vast worldwide networks of electronic data.

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, and organizations must therefore 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, if possible, to reach agreement concerning 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. When the responding party has shown that it has acted reasonably to preserve and produce relevant electronic data and documents, the burden should be on the requesting party to show that additional efforts are warranted under the circumstances of the case.

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, and 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 properly access and identify potentially responsive electronic data and documents by using reasonable selection criteria, such as search terms or samples.

12. Absent specific objection, agreement of the parties or order of the court, electronic documents normally include the information intentionally entered and saved by a computer user.

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, it is found that there was an intentional or reckless failure to preserve and produce relevant electronic data, and a showing of a reasonable probability that the loss of the evidence materially prejudiced the adverse party.

Principles and Comments

1. Electronic data and documents are potentially discoverable under Fed. R. Civ. P. 34 or its state law equivalents, and organizations must therefore properly preserve electronic data and documents that can reasonably be anticipated to be relevant to litigation.

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

Organizations should adopt policies that provide rational and defensible guidelines on the treatment of electronic documents. These guidelines should be set with reference to the business, regulatory, and tax needs of the organization, including the need to conserve electronic storage space on e-mail servers. Thus, a company that determines it only needs to retain e-mail with business record significance could set these guidelines forth in its document retention policy. Employees would then be charged with responsibility 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 anticipated discovery. The existence and reasonable effectiveness of such a program should be a significant consideration in any spoliation analysis.[13]

The advantages of a document retention policy are particularly pronounced with respect to backup tapes and hard drives. An effective document retention policy, 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 backup tapes or hard drives. Under such a policy, backup tapes and hard drives would not be governed by an inaccurate characterization of them as retention systems, but rather by a proper understanding of their role in providing for system reconstruction in the event of loss of functionality.[14]

An appropriate electronic document preservation program would involve most or all of the following:

- Establishment of a thorough but practical records management program and training of individuals to manage and retain business records created or received in the ordinary course of business;
- 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-mails that are not business records and develop communications policies that promote the appropriate use of the e-mail and other company-owned systems;
- Structuring the recycle time applicable to backup tapes based on business 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 pending litigation; and
- Establishing and maintaining awareness of the importance of the preservation of potential evidence in the case of threatened litigation, and training lawyers and business people on when and how to carry out their responsibilities.

---

13 Absent assigning one "records guardian" to oversee each employee, no organization can ensure 100% percent compliance with its records management program.

14 Unlike archival systems, which contemplate restoring data, in part or whole, to an existing, active system to be used along with other active data, backup systems are designed to completely restore active systems that have been lost or corrupted as the result of some disaster. Therefore, while data stored in offline archives may often be restored to the active system and searched, searching backup files often requires either taking active data off the system or 'cloning' the system. Both alternatives involve significant disruptions and expense.

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.[15] 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. Preservation in the Context of Litigation

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 these obligations, however, all organizations must remain cognizant of preservation obligations related to litigation. Discerning when the obligation attaches (and the scope of the obligation) involves a highly fact-specific inquiry. Failure to properly preserve documents can lead to serious consequences in litigation. *See Metro. Opera Ass'n. v. Local 100, Hotel Emples. & Rest. Emples. 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).

> *Illustration i.* Acme Pharmaceutical Co. ("Acme") manufactures an antacid that is marketed under the name Doxin. On April 1, it receives a letter from Consumers' Laboratory, a consumer rights group, which states that Consumers' Laboratory intends to bring a suit alleging that patients who use Doxin have an increased risk of stroke or heart attack. Upon receipt of the letter, Acme can reasonably anticipate litigation and begins preserving all documents related to Doxin.
>
> *Illustration ii.* Big City Automotive Parts ("Big City") manufactures radiators. It has never received any complaints regarding the quality of its radiators, and it has conducted surveys of mechanics indicating that Big City radiators perform as well or better than competitors' radiators. On September 15, Big City is served with a complaint in a class-action lawsuit on behalf of all persons who purchased cars with Big City radiators between 1990 and 2001. The complaint alleges the radiators are defective. Because Big City could not have reasonably anticipated the suit prior to receiving the complaint, its preservation obligation is not triggered until service of the complaint.

[15] Thus, for example, in *Lewy v. Remington,* 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 had been filed, the frequency of such complaints, the magnitude of the complaints, and whether the retention policy had been implemented in bad faith.

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. Discovery of Electronic Documents Under the Federal Rules

Federal Rule of Civil Procedure 34 permits the service by one party upon another of a request for documents in any format:

> Any party may serve on any other party a request (1) 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, phone records, 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[.]

The Notes to the 1970 Amendment to Rule 34 explain that electronic documents may be requested:

> 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, and that when the 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 non-discoverable matters, and costs.

See also Anti-Monopoly, Inc. v. Hasbro, Inc., 94 CIV 2120, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995) ("It is black letter law that computerized data is discoverable if relevant"); *Bills v. Connect Corp.,* 108 F.R.D. 459 (C.D. Utah 1985) (information stored in computers should be freely discoverable as information not stored in computers). *Cf. Simon Property Group L.P. v. my Simon,* 194 F.R.D. 639, 640 (S.D. Ind. 2000) ("[C]omputer records … are documents discoverable under Fed. R. Civ. P. 34.").

Discovery of electronic documents, however, is not without limits. The Notes to the 1970 Amendment to Rule 34 also point out that the courts have power under Rules 26(b)(2) and 26(c) to limit discovery:[16]

> 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: (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) 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.

[16] Although the 1970 Committee Notes only mention Rule 26(c), courts frequently place more reliance on Rule 26(b)(2) in limiting discovery.

> Upon motion by a party or by the person from whom discovery is sought, accompanied by a certification that the moving party 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[.]

This broad power enables a court to limit discovery of electronic documents or condition their production on cost shifting in those cases where the court concludes that the burden of the discovery outweighs its ultimate benefit.

Comment 2.b. Scope of Reasonable Inquiries

The traditional approach to preserving and producing paper documents has been to locate 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 facilitate gathering and producing documents, after review for privilege, trade secrets, or other appropriate bases for non-production. A similar approach is also proper for persons who may have relevant information in electronic format. The Federal Rules of Civil Procedure 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.

Comment 2.c. 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 must be converted into text to be understood, 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, or transaction costs due to electronic discovery will overwhelm the ability to resolve disputes fairly in litigation. *See, e.g., Alexander v. Federal Bureau of Investigation,* 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 of Civil Procedure to determine that benefits of discovery outweigh expense).

It is important to recognize that costs cannot be calculated solely in terms of the expense of computer technicians to retrieve the data, but must also factor in other litigation costs. For instance, the court in *In re General Instrument Corporate 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 back-up 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.d. Need to Coordinate Internal Efforts

Decisions regarding the preservation of electronic documents and data is typically a team effort, involving counsel (inside and outside), information systems professionals, end-user representatives, records management personnel, and potentially other groups with knowledge of the relevant computer systems and how data is used, such as internal audit or information security personnel. Outside consultants may be used, and are included in some of the team activities when consistent with the need for privileged communications. The team approach permits the 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 at issue.

Comment 2.e. Communications with Court Regarding Electronic Data Collection

Organizations should maintain reasonable positions when presenting electronic data collection issues in court. The organization should be clear that it intends to fulfill its responsibility to preserve and produce data needed for fair adjudication of the case. Overstated or excessive cost estimates will reduce the organization's credibility. Where feasible, the organization should move forward early in litigation with a fair and reasonable plan for collecting and producing data, rather than leaving the court to rule on competing plans. When providing affidavits or testimony to the court on these issues, the organization should take note that judges and juries 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 and seek when these matters are at issue in the litigation, if possible, to reach agreement concerning 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

Given the degree of differences among computer systems and practices with respect to electronic information, it is clearly in the interest of the parties to clarify early in discovery exactly what will and will not be at issue. In fact, several United States District Courts have, via local rule, mandated such conferences. *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 include a variety of details on electronic discovery as specified by the rule."); U.S. Dist. Ct. Wyo. L. R. 26.1(d)(3)(a) ("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."). The Rule 26(f) conference is an important tool that can enable the parties to preempt disputes regarding the discovery of electronic documents. By discussing such issues 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 at the onset of a case, 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. 437 (D.N.J. 2002) (noting importance of discussing electronic evidence at Rule 26(f) conference). Checklists of key issues to be considered during an electronic discovery conference can provide helpful guidance to the parties. Requiring the parties to frame open issues also allows the court to intervene where necessary with appropriate methods of resolving disputes and thereby minimizes post-discovery spoliation disputes. *See id.* (where party possesses relevant information in electronic format, it is obligated to advise adversary under mandatory disclosure rules); *Kleiner v. Burns,* 48 Fed. R. Serv. 644 (D. Kan. 2000) (holding that Rule 26 requires disclosure of nature and location of relevant electronic documents).

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 or the need to 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 brokerage houses 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 preservation of existing data, including the preservation of select (not all) back-up tapes, certain archived data, select legacy systems, distribution of retention notices (and updates), a limited number of "mirror images" to be made for select computer hard drives, measures to be undertaken to collect potentially relevant data, and 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 motions practice and provides certainty as to the expected preservation efforts. *Cf.* Electronic Data Preservation Protocol in *In Re Initial Public Offering Securities Litigation,* 21 MC 92 (SAS) (S.D.N.Y. Dec. 2002).

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 considered by the producing party in responding to document requests should do so 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 and instead target particular electronic data that the requesting party contends is important for the resolution of the case. The requesting party may elect to identify the form in which it wishes the data to be produced.

When the requesting party has knowledge of specific attributes of the responding party's computer systems, that knowledge should inform and shape the discovery requests. Such an approach avoids unnecessary confusion regarding what is being asked for, and enables the parties to better frame areas of disagreement. *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. To the extent that production has not been made from all reasonably available sources of electronic documents and data, a respondent should tender appropriate objections based upon cost, burden, overbreadth of the request or other factors. It is neither reasonable nor 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 produce data from active files on computers and readily accessible archival media such as floppy disks, ZIP drives or CDs, rather than retrieve data from backup tapes.

Comment 4.c. Disclosure of Collection Parameters

It is usually not feasible, and may not even be possible, for most 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 would in nearly every lawsuit literally cripple 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 by discussion of the potential scope and costs of collecting relevant data with the party seeking discovery.

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, it is incumbent upon organizations to take reasonable steps to preserve electronic documents for litigation, whether pending or reasonably anticipated.

However, the obligation to preserve relevant evidence is generally understood to require on the part of the producing party only 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 through applications of various computer systems. If such overwriting is incidental to the operation of the systems, it should be permitted to continue after the commencement of litigation. *See* Martin C. 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"). Striking that balance in the context of routine operating systems that are intended, in good faith, to operate continuously presents special problems that should be addressed with care.

> *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. 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 systems is to assist the organization in its business or other designated activities. Organizations cannot realistically consider the ability to respond efficiently to discovery requests in designing, configuring or using all of their systems. Nonetheless, the need to respond to discovery in litigation is a fact of life for many organizations. The costs of responding to 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 collect, store, review, and produce data that may be responsive to discovery requests or required for initial mandatory disclosures. Preparation 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.

A document retention policy can be a vital tool to an organization to better manage its electronic documents. By creating and implementing a policy that sets forth the organization's policies on the management and retention of electronic documents, an organization can realize several benefits. First, adherence to a document retention policy helps ensure that the organization will not retain outdated or irrelevant documents. Second, if a responding party can, during discovery disputes, direct the courts and the requesting party to a pre-existing document retention policy, the responding party can objectively and credibly account for any documents it may have destroyed pursuant to that policy prior to the onset of litigation. *See Lewy v. Remington Arms Co.,* 836 F.2d 1104 (8th Cir. 1988) (remanding case to trial court with instructions to consider whether defendant's records retention policy was reasonable).

> *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 a 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.

Illustration ii. Pursuant to a records management policy, a producing party requires its employees to limit the quantity of electronic information that is stored or the time that communications that do not constitute records of the organization can remain in the employees' respective active e-mail accounts. Upon commencement of litigation, adequate steps are taken to inform the appropriate individuals to save relevant electronic data now and in the future, and reasonable procedures are implemented to ensure compliance by individuals with potentially relevant documents. The organization should not be required to suspend the routine deletion of other electronic data in accordance with its records management policy.

Comment 5.c. Corporate Response Regarding Litigation Preservation

Ordinarily, organizations should take steps to 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.

In addressing preservation issues, an organization needs to understand that 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. That said, organizations addressing the 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 (N.D. Ill. Dec. 18, 2002) (Court required company to "research their tapes under the broader subject matter and time period" ordered in the case). Ideally, an effective means of retention and compliance of the documents reasonably subject to the preservation obligation should be established as soon as practicable and an appropriate notice should be effectively communicated to an appropriate list of affected persons. (*See* Comment 5.d, *infra.*) Involvement of senior management or legal advisors in the retention decisions and processes may be required, depending upon the particular circumstances involved. *Cf. In re Prudential Ins. Co. of Am. Sales Practices,* 169 F.R.D. 598, (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 sanction); *see also Danis v. USN Communications,* 2000 WL 1694325 (N.D. Ill. 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 trigged a preservation obligation, the organization should take reasonable steps to communicate to affected persons the need for and scope of preservation of records (both electronic and hard copy) relevant to the matter. The form, content and distribution of the notice may and will vary widely between and among organizations depending upon the circumstances, and there is no talisman.

The notice need not be, and most likely should not be, a detailed catalog of information types to be retained but instead should provide a sufficient description of the kinds of information subject to preservation that would allow the affected custodians of data to segregate and preserve identified files and data. The notice should state that electronic as well as paper documents are subject to the preservation request. Consideration should be given whether the notice should specifically address preservation of data in multiple locations (*e.g.,* network, workstation, laptop or other devices), with a final determination

depending significantly 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. The breadth of the communication need not extend beyond the scope of reasonable inquiry absent specific information and knowledge that requires otherwise.

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.[17]

> *Illustration i.* Pursuant to its procedures for litigation response, the organization identified the departments and employees involved in the potential dispute with a vendor. Those individuals whose files are reasonably likely to contain documents that may be relevant to the subject matter of the potential dispute are notified via e-mail and hard copy memorandum of the potential dispute and are asked to take steps to retain documents (including electronic records) that may be relevant to the subject matter (which is generally described in the communication). The organization also reviews the shared and system data available to determine if any steps need to be taken with computer systems administrators to copy or isolate data for preservation.

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 frames a party's obligation in terms of the "possession, custody or control" of documents. If an organization uses a third party to host data that is not otherwise on the premises, the organization should consider whether notice must be provided to the third party to preserve affected data. Inherent in these considerations is an understanding of the nature and potential relevance of data held by a third party. It is also important for the responding party to set forth any objections to reviewing a producing 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. *Cf.* ABA Discovery Standard, 29(a)(iii) ("[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."). 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 should be exercised and the extraordinary efforts should be required 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

[17] When preservation obligations extend over documents and data spanning a significant or continuing time period, organizations should analyze any need to review and catalog hardware that is being retired where there is also a reasonable likelihood that the hardware contains unique relevant documents.

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."). Preservation orders should be issued only after the court conducts a hearing to determine the scope of the electronic information sought, the efforts that have already been undertaken to produce the requested information and the effort required to fully comply with the requests. Courts should not order unreasonable or unduly burdensome tasks.

> *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 the necessity of such an order. Because all litigants are obligated to preserve documents in their possession, custody, or control that are relevant to the litigation, 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 Prod., Inc.,* 187 F.R.D. 636, 642-43 (S.D. Cal. 1999) (denying motion for preservation order because of the technical difficulties of permanently destroying electronic documents); *Gorgen Co. v. Brecht,* No. C2-01-1715, 2002 WL 977467, at *3 (Minn. Ct. App. May 14, 2002) (overturning temporary restraining order barring defendants from destroying or altering 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. Prior to the issuance of a preservation order, 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 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. *Ex parte* 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, 1994 WL 1108312, at *7-8 (D. Minn. Dec. 5, 1994) (applying standard for injunctive relief to request for a preservation order); *Humble Oil & Ref. 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. Serv., Inc. v. Riley,* 105 Cal. App.4th 1414, 2003 WL 245586 (Cal 4th App. Dist. Feb. 5, 2003) (applying standards for injunctive relief to request "to 'freeze' Defendants' electronically stored data.") In most instances, neither a 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 electronic mail. 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 untoward statements or conduct. Yet, the burdens and costs of those acts are apparent and no one would 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 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. In this context, imposition of an absolute requirement for preservation of all information would require shutting down all computer systems and making copies of each and every bit of data on each fixed disk drive, as well as any other media that are normally used by the system. Costs of litigation would routinely approach or exceed the amount in controversy in most lawsuits if such an approach were to be required. In the ordinary course, 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 in *Landmark Legal Foundation v. EPA,* No. 00-2338 (D.D.C).

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 of Civil Procedure do not require such a search, and the handful of cases are idiosyncratic and provide little guidance.").

In some organizations, 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 archived. Backup tapes may also be retained for long periods of time out of concern for compliance with record retention laws. 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. Organizations seeking to preserve data for business purposes or litigation should, if possible, employ means other than disaster recovery backup tapes. Alternatives include utilizing copies of relevant files, "snap" server copies, and targeted archive tape creation.

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.

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 data belonging to any specific employee. Any such areas containing potentially relevant data should be identified promptly and appropriate steps taken to preserve shared data that is determined to be subject to a preservation obligation. Where 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 notification of persons responsible for management of 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 or is not responsive to discovery demands and to make adequate arrangements to preserve and produce the information. Organizations should identify and define preservation obligations at the outset of litigation. 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.,* 53 Fed. R. Serv. 3d 828, 2000 WL 1694325, at *37-38 (N.D. Ill., Oct. 20, 2002) (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 information that may be relevant to the dispute at issue. 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 intrusive efforts beyond these merely because the party seeking discovery is suspicious of or concerned about the quality of the efforts undertaken by the producing party. *See McCurdy Group v. American Biomedical Group,* 9 Fed. Appx. 822, 831 (10th Cir. 2001) (affirming denial of motion to compel production of hard drives based on fact that party seeking discovery was "skeptical" that all relevant and non-privileged documents had been produced).

> *Illustration i.* Johnson Manufacturing Co. ("Johnson") receives discovery in a lawsuit and takes steps to preserve documents. It enlists the assistance of its employees or agents who are identified as possibly having relevant information by informing them of the nature of the controversy and the time frame involved, and by providing them with a method of accumulating and updating (where disputes are ongoing) copies of the relevant information for production. The individuals are instructed on the necessity of preserving relevant information (this instruction is sometimes referred to as a "litigation hold order"), including the information available to them in their active e-mail and other electronic formats, and steps are established to secure the information. Johnson has met its preservation obligations.

Comment 6.b. Scope of Electronic Data Collection

When responding to discovery requests, organizations should take the initiative in defining the scope of the data needed to address appropriately and fairly 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 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 Benton v. Allstate Ins. Co.,* 2001 WL 210685, at *7 (D. Cal. Feb. 26, 2001) (granting summary judgment to defendant despite plaintiff's claim that he needed to conduct discovery of defendant's computer system where plaintiff had provided no evidence that information on computer system would be relevant to issues raised in the motion for summary judgment); s*ee also Fennell v. First Step Designs, Ltd.,* 83 F.3d 526, 532 (1st Cir. 1996) (affirming order denying electronic discovery where that discovery would be a "fishing expedition."); *Stalling-Daniel v. The Northern Trust Co.,* 52 Fed. R. Serv. 3d 1406, 2002 WL 385566, at *1 (N.D. Ill. Mar. 12, 2002) (denying a request by plaintiff for an order permitting an expert

to conduct an intrusive and detailed examination of discovery of defendant's systems 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.

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. If a party is permitted to perform a Rule 34 inspection, such an inspection:

a) may encompass and invade trade secrets;
b) may encompass other highly confidential information, including materials, such as personnel evaluations and payroll information, properly private to individual employees;
c) may encompass and invade confidential attorney-client communications and other confidential material prepared and organized by the party's attorneys;
d) would massively disrupt and could even halt the ongoing business; and
e) if file-recovery software is permitted to be used, it could corrupt operating systems, software applications, and electronic files.

In order 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 narrowly restricted to protect confidential information and system integrity and to avoid giving the discovering party access to data unrelated to the litigation. *See generally Van Westrienen v. Americontinental Collection Corp.,* 189 F.R.D. 440 (D. Or. 1999) (producing party has right to review files before production, whether in electronic or paper format). Further, no inspection should be permitted to proceed until the producing party has had a fair opportunity to review the data subject to inspection. However, where the required showing is made, the data subject to inspection may be obtained exigently and so as to preserve the producing party's rights, for example, through the use of "neutral" court-appointed consultants. *See* Comment 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. 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.

See Gates Rubber Co. v. Bando Chemical Indus., Ltd., 167 F.R.D. 90, 121 (D. Colo. 1996). 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 and reliability of the vendor.

Comment 6.e. Documentation and Validation

In developing data collection procedures, organizations should consider the appropriate scope for 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 and is not 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 utilizes 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. When the responding party has shown that it has acted reasonably to preserve and produce relevant electronic data and documents, the burden should be on the requesting party to show that additional efforts are warranted under the circumstances of the case.

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 for production. 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) ("Plaintiff's 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

Where the responding party makes a showing that it has acted reasonably to preserve and produce electronic data and other documents, courts should balance the cost, burden and need for imposing on third parties who may copies of such documents when confronted with requests to obtain the same or similar materials from third parties under Rule 45 of the Federal Rules of Civil Procedure. *See Braxton v. Farmer's Ins. Group,* 203 F.R.D. 651 (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).

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, and 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 and include locations reasonably likely to contain active and purposefully stored information. Potentially relevant information may be found in local and network computers, archive and backup data tapes, laptop computers, handheld storage devices (such as PDAs), 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.

Comment 8.b. Forensic Data Collection

The proper subject of discovery is electronic data and documents that are relevant to the claims and defenses in the case, and a requesting party should not be permitted to discover electronic data and documents that do not meet this standard regardless of how technically feasible access may be. Accordingly, forensic data collection should not be required unless exceptional circumstances warrant the extraordinary cost and burden of this approach. *See McPeek v. Ashcroft,* 212 F.R.D. 33, 36 (D.D.C. 2003) (declining to order searches of backup tapes where the burden on defendant in searching those tapes would be great and plaintiff had not demonstrated a likelihood of obtaining relevant information). Making 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 other business purposes. In contracting for such services, organizations should consider whether there is provision for the types of activities, such as preservation or collection of data that may be required by electronic discovery. 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. If an organization uses a third party to host data that is not otherwise on premises, the organization should consider whether notice must be provided to the third party to preserve affected data.

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 compilation" as included in Rule 34 was intended to turn *all* forms of "data" into a Rule 34 "document." *Cf.* The Hon. Shira A. Scheindlin and 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.' Certainly they are not 'documents' in any traditional sense"; article thereafter posits that notwithstanding the nomenclature, such information "represents a potentially fruitful means by which litigants may discover important facts").[18]

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 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 "document." Nor should data that is not accessible except through forensic means, such as deleted or residual data. 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 (D.D.C. 2001) (court rejected notion that there is an absolute obligation to pursue potentially relevant data on backup tapes); *McPeek v. Ashcroft,* Civ. A. No. 00-201 2003 WL 75780 (D.D.C. Jan. 9, 2003) (rejecting plaintiff's demand for additional searches of backup tapes); *In re Brand Name Prescription Drugs Antitrust Litig.,* Nos. 94 C 897, MDL 997, 1995 WL 360526 (N.D. Ill. June 15, 1995) (producing party obligated to produce electronic data). 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.").

---

[18] There are few analogues in the paper world for the many variations and aspects of "data" seen in the electronic age. One apt analogy is the typewriter ribbon — from which it may be possible to reconstruct the content of a letter in certain circumstances. Does the ability to reconstruct "evidence" make the typewriter ribbon a "data compilation" or a "document"? The better answer is "no." It may be a discoverable (and even admissible) "thing" in the proper case, but it should not be treated as a "document."

As a legal matter, the distinction makes no difference. Both "documents" and "things" are discoverable under Rule 34. Yet the distinction could well prove valuable from a practical standpoint as litigants and courts can separately address the need for and relevance to claims and defenses of data "readily compiled into information" (*i.e.,* "documents") as opposed to data that are hidden or not accessible except through forensic means (*i.e.,* "things"), such as deleted or residual data.

Illustration i. A party demands that responsive documents, "whether in hard copy or electronic format," be produced. The producing party assembles copies of the relevant hard copy memoranda, prints out copies of relevant e-mails and electronic memoranda and combines them into a PDF format on a read-only CD-ROM that does not include metadata that is not seen or accessed by the user. 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 venture capital transaction, based upon an e-mail allegedly sent by the president of defendant corporation, a venture capital firm, 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 clearly 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 or not the questioned message is authentic.

Illustration iii. Plaintiff alleges that the defendant engaged in fraud regarding software development. The plaintiff sets forth evidence showing that the computer program sold by defendant appears to incorporate plaintiff's source code. Plaintiff sets forth 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, preservation obligations should not extend to deleted data 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 is typically the case, deleted data 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 to the matters in question will be marginal at best in most cases, while the burdens involved will be great. In exceptional cases, however, there may be good cause for targeted preservation of deleted and residual data.

In addressing the issue of deleted and residual data, it is important to recognize that such data, like papers discarded in a trashcan, is subject to potential 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, 427-431 (S.D.N.Y. 2002) (stating that "[e]lectronic documents are no less subject to disclosure than paper records," and only questioning which party should bear the cost of such discovery, especially for backup tapes or deleted e-mails); *McPeek v. Ashcroft,* 202 F.R.D. 31, 34 (D.D.C. 2001) (stating that, "[d]uring discovery, the producing party has an obligation to search available electronic systems for information demanded," and ordering a limited backup restoration of e-mails); *Kleiner v. Burns,* 48 Fed. R. Serv. 3d 644, 2000 WL 1909470, at *4 (D. Kan. Dec. 15, 2000) (noting that Rule 26(a)(1)(B) requires description and categorization of computerized data, including deleted e-mails, and stating that "[t]he disclosing party shall take reasonable steps to ensure that it discloses any backup copies of files or archival tapes that will provide information about any 'deleted' electronic data"); *Simon Property Group L.P. v. mySimon, Inc.,* 194 F.R.D. 639, 640 (S.D. Ind. 2000) ("First, computer records, including records that have been 'deleted,' are documents discoverable under Fed. R. Civ. P. 34."); *Playboy Enter. v. Welles,* 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999) ("Plaintiff needs to access the hard drive of Defendant's

computer only because Defendant's actions in deleting those e-mails made it currently impossible to produce the information as a 'document.'").

However, it is the exceptional case that will turn on "deleted" or "discarded" information (whether paper or electronic) and the 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. August 29, 1997) ("Fourteen days worth of e-mail, which might contain a few deleted e-mail, 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 Fisher e-mail."); *Strasser v. Yalamanchi,* 669 So. 2d 1142, 1144 (Fla. Ct. App. 1996) ("Even if plaintiff represents accurately that defendant has been thwarting the discovery process, such conduct does not necessarily invite intrusive discovery where there has been no evidence to establish any likelihood that the purged documents can be retrieved.").

> *Illustration i.* A party seeking relevant e-mails demands that a search be made of inactive accounts, backup tapes, and hard drives for deleted materials. No showing of special need or justification is made for the extraordinary search. The request should be denied. *See Moore's Federal Practice* § 37A.32[3][c] ("If forensic computer assistance is employed to restore deleted files or if the number of files to be searched is large, a mirror image of the computer's hard drive is likely necessary and the recovery costs can be substantial. Alternative ways of producing the requested information may be feasible and should be explored."). No more duty exists to preserve and produce deleted electronic information after commencement of litigation than exists to sequester and search the trash bin outside an office building.
>
> *Illustration ii.* After departure of a key employee from X Company ("X Co.") to 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, burning the data to 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 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

Because of the large volumes of documents and data typically at issue in cases involving production of electronic data, 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 approach the court for entry of an appropriate non-waiver order. 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 prior to any production.[20]

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

Special issues may arise with any request to inspect a computer system. In particular, 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 a third-party expert. *See Simon Property Group L.P. v. mySimon, Inc.,* 194 F.R.D. 639, 642 (S.D. Ill. 2000) (using appointed expert/vendor operating under constraints of protective order). Similar concerns exist regarding the potential disclosure of attorney-client privileged or work product information, and there is no guarantee that a non-waiver order in one jurisdiction will be fully honored in another in the event of the disclosure or release of protected information. Accordingly, court-ordered inspections of computer systems should be sparingly used and, when done, should be narrowly tailored to the circumstances and accompanied by a sufficient protective order.

---

[19] An illustrative example is in the *Bridgestone/Firestone/Ford* multi-district litigation currently pending in 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.*

[20] Counsel should understand, however, that such an order will not provide absolute protection in the event of repeated productions of the same documents.

11. A responding party may properly access and identify potentially responsive electronic data and documents by using reasonable selection criteria, such as search terms or samples.

Comment 11.a. Key Word Searches

Litigants should discuss specific criteria, including search terms, to be used in searches of electronic data for production. 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. Selective use of key concept and word searches is a reasonable approach when dealing with large amounts of electronic data. *Cf.* Prac. Guide Fed. Civ. Prac. Before Trial, 5th Cir., Ch. 11-H(3)(A)(3). 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. Courts should encourage and promote the use of such techniques in appropriate circumstances, which can, in part, be identified by sampling techniques. *See McPeek v. Ashcroft,* 202 F.R.D. 31, 35 (D.D.C. 2001) (ordering production of e-mails from a limited time period from the computer of a single user); *Tulip Computers Int'l B.V. v. Dell Computers Corp.,* No. Civ.A. 00-981-RRM, 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.").

The scope of terms employed must be reasonably calculated to return the requested 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" Litigation,* No. 01 C 2963, 2002 WL 31844956 (N.D. Ill. Dec. 18, 2002), the court found that the defendants' document production efforts, which involved word searches on twenty-five 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. *But see McPeek v. Ashcroft,* No. Civ. A. 00-201, 2003 WL 75780 (D.D.C. Jan. 9, 2003) (rejecting plaintiff's demands for additional searches of backup tapes based upon burden and limited likelihood that relevant information could be retrieved from additional searches).

> *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 utilizes 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. 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 selection of items that are potentially relevant to a given litigation, whether by the document authors or custodians themselves, litigation support or information services personnel, or others. In a manual collection, the items may be copied or transmitted by the end-user. Automated collection involves use of automated archiving programs 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/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, however, consistency across the production can help ensure that responsive documents have been produced as appropriate.

12. Absent a specific objection, agreement of the parties or order of the court, electronic documents normally include the information intentionally entered and saved by a computer user.

Comment 12.a. Metadata

An electronic document can include not only the visible text but also hidden text, formatting, 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 documents (for example, the proper fonts, spacing, size and color). 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. Rarely is this information critical to the resolution of a dispute. When a document is printed (or saved in an image format), much of the "display" of the document is preserved, but not the underlying data.

There should be a presumption that most cases will not require any special care, preservation or production regarding metadata. While the potential of relevance and need for metadata exist, it is likely to remain the exceptional situation in which metadata is produced, and metadata should therefore not drive courts' analyses. *See Munshani v. Signal Lake Venture Fund II, LP,* 13 Mass.L.Rptr. 732, 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).[21] However, litigants and courts may need to scrutinize the claims and defenses in a particular case before making a final determination regarding the retention and production of metadata. Further, 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.

Comment 12.b. Formats Used for Collecting Data

Data can be collected in its original format or can be converted to an image (such as .TIF file or paper printout). Conversion increases the cost of collection, but may be more consistent with downstream review procedures familiar to counsel and can simplify the process of redacting text from documents. Conversion may also cause loss of metadata. The appropriate format for collection should be determined after considering the nature of the litigation for which the data is being collected.

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

Electronic data should be produced in a form that preserves the substantive information content 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, production of electronic data in a commonly accepted image format (paper, .PDF or .TIF) should be sufficient in most cases. Similarly, absent specific objection, agreement of the parties or order of the court, data that is not ordinarily viewable or printed when performing a normal print command need

---

[21] In a number of ways, much of the information that could be retrieved from metadata is further removed (in terms of relevance and need) from the information that can be retrieved from paper copies of draft letters and memoranda. Moreover, there is good authority supporting the proposition in that paper world the utility (and thus need and value) of drafts is limited to the rare case where resort to a draft document is 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 testing 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); *see also Alexander v. FBI,* 194 F.R.D. 305, 309 (D.D.C. 2000) (denying motion to compel production of drafts).

not be produced. In a growing number of cases, it may be preferable and more cost effective for the production to occur in electronic format. Whatever format is chosen should be one that allows 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., In re General Instrument Corp. Sec. Litig.,* No. 96 C 1129, 1999 WL 1072507 (N.D. Ill. Nov. 18, 1999); *McNally Tunneling v. City of Evanston,* No. 00 C 6979, 2001 WL 1568879 (N.D. Ill. Dec. 10, 2001). If a court does require reproduction of documents already produced once, the court should shift 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).

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. Cost-Shifting

The ordinary and predictable costs of discovery are fairly borne by the producing party, although Rule 26(b) clearly empowers courts to shift costs where the demand is unduly burdensome because of the nature of the effort involved to comply. Thus, where a court requires efforts to retrieve information beyond that which is reasonably available, it should also adjudicate the need for cost shifting in the individual case. *See Rowe Entm't, Inc., et al. v. The William Morris Agency, Inc., et al.,* 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 (including deleted data, disaster recovery backup tapes, residual data and legacy systems and tapes) should be allocated to the requesting party.

The *Rowe* court laid out eight factors to be used 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 understand the circumstances under which the expenses of discovery exceed those that a responding party should reasonably be expected to bear. *See also ABA Discovery Standard,* 29(b)(iii) ("The discovering party generally should bear any special expenses incurred by the responding party in producing requested electronic information."); 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."); *Murphy Oil USA, Inc. v. Flour Daniel, Inc.,* 52 Fed. R. Serv. 3d 168 (E.D. La. 2002) (applying *Rowe* factors).

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. The Northern Trust Co.,* 52 Fed. R. Serv. 3d 1406, 2002 WL 385566, at *1 (N.D. Ill. Mar. 12, 2002) ("Nothing in the documents produced justifies an intrusive and wholly speculative electronic investigation into defendant's e-mail files."). 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.

> *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 producing party seeks a protective order conditioning its production upon payment of costs, including the costs of review. *See* Tex. R. Civ. Pro. 196.4, *supra.* 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, it is found that there was an intentional or reckless failure to preserve and produce relevant electronic data, and a showing of a reasonable probability that the loss of the evidence materially prejudiced the adverse party.

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

Due to the complexity of modern computer systems, large volumes of electronic data and continuing changes in information technology, the potential for good faith errors or omissions in the process of preserving and producing electronic information will always exist. 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. A spoliation finding should require the existence and 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 (RLC)JCF, 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). *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, only when specific restrictions upon operating systems are sought and, if objected to, required by order, should the court impose sanctions for non-production. *But see Linnen v. A.H. Robins Co.,* 1999 Mass. Super. LEXIS 240, at *36 (Mass. Super. Ct. June 15, 1999) (obligation to cease recycling of backup tapes arose by inference after *ex parte* order governing same was lifted). However, the failure to take reasonable steps to ensure a good faith effort to preserve relevant electronic data may lead to spoliation instructions or other sanctions. *See Residential Funding Corp. v. DeGeorge Financial Corp.,* 306 F.3d 99, 107-08 (2nd Cir. 2002) (imposing sanctions for negligent failure to take adequate steps to preserve and produce documents in a timely manner); *Lexis-Nexis v. Beer,* 41 F. Supp. 2d 950, 955 (D. Minn. 1999) (imposing sanctions for destruction of relevant database). Untimely challenges of non-production of information should not, however, support a motion for sanctions. *Allen Pen Co. v. Springfield Photo Mount Co.,* 653 F.2d 17, 23 (1st Cir. 1981).[22]

> *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 sanctions.

[22] It must be recognized that 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 107-08 [emphasis supplied].

Comment 14.b. Prejudice

A party seeking sanctions should be required to meet the burden of proving that there is a reasonable likelihood the party has been materially prejudiced by the complained of act. *See Concord Boat Corp. v. Brunswick Corp.,* No. LR-C-95-781, 1997 WL 33352759, at *6 (E.D. Ark. Aug. 29, 1997) (holding that destruction of e-mail with "tangential relevance" would not justify imposition of sanctions); *see also 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); *Seattle Audubon Soc'y. v. Lyons,* 871 F. Supp. 1291, 1308-9 (W.D. Wash. 1994) (District court would not presume that documents destroyed by government were adverse to government, absent showing that government had notice that documents were relevant in action challenging validity of forest management plan; employees were told to retain material documents, but were left free to discard others, largely in their discretion, and there was no proof of any ulterior motive); *cf. Residential Funding Corp. v. DeGeorge Financial 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 thousands or even millions of files and messages. Given the volumes of data involved, such processes cannot be perfect, 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.

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 Recycling: Backup Tape Recycling describes the process whereby an organization's backup tapes are overwritten with new archived 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 are data that, in the past, existed on the computer as live data and which have been deleted by the computer system or end-user activity. Deleted data remain on storage media in whole or in part until they are overwritten or "wiped." Even after the data itself have 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 Tapes: 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 of Civil Procedure.

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.

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 the development of which an organization may have invested significant resources and has retained its importance, but 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 describes how, when and by whom it was collected, created, accessed, 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 not highly informative "short hand" phrase "data about data," describing the content, quality, condition, history, and other characteristics of the data.)

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.

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.

Sampling: Sampling usually (but not always) refers to the process of statistically testing a database for the likelihood of relevant information. It can be a useful technique in addressing a number of issues relating to litigation, including decisions what repositories of data are appropriate to search 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:
Working Group Participants & Observers

Sharon A. Alexander, Esquire
Jones Day
Participant

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

Thomas Barnett, Esquire
Electronic Evidence Discovery, Inc.
Participant

Steven C. Bennett, Esquire
Jones Day
Participant

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

The Honorable John L. Carroll (ret.)
Cumberland School of Law
Samford University
Observer

Barbara Caulfield, Esquire
Affymetrix, Inc.
Participant

Cynthia S. Cecil, Esquire
Hunton & Williams
Participant

R. Noel Clinard, Esquire
Hunton & Williams
Participant

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

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

Robert A. Eisenberg
Peterson Consulting
Participant

Jason Fliegel, Esquire
Mayer Brown Rowe & Maw
Participant; Editor

Sherry B. Harris
Hunton & Williams
Participant

Gary L. Hayden, Esquire
Ford Motor Company
Participant; Steering Committee

Ted S. Hiser, Esquire
Jones Day
Participant; Editor

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

John H. Jessen
Electronic Evidence Discovery, Inc.
Participant; Steering Committee

Jeffrey J. Joyce, Esquire
Jones Day
Participant

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

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

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

James L. Michalowicz, Esquire
DuPont
Participant

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

Timothy M. Opsitnick, Esquire
JurInnov Ltd.
Participant

Ashish S. Prasad, Esquire
Mayer Brown Rowe & Maw
Participant; Senior Editor

Charles R. Ragan, Esquire
Pillsbury Winthrop LLP
Participant

Jonathan M. Redgrave, Esquire
Jones Day
Participant; Steering Committee;
Editor-in-Chief

Dan Regard, Esquire
FTI Consulting, Inc.
Participant

Mark V. Reichenbach
Pillsbury Winthrop LLP
Participant

Paul M. Robertson, Esquire
Bingham McCutchen LLP
Participant

Leigh R. Schachter, Esquire
Debevoise & Plimpton
Participant

Kenneth Shear, Esquire
Electronic Evidence Discovery, Inc.
Participant

Lori Ann Wagner, Esquire
Faegre & Benson LLP
Participant

Megan A. Walker
Ford Motor Company
Participant

Robert F. Williams
Cohasset Associates, Inc.
Participant

Kenneth J. Withers, Esquire
Federal Judicial Center
Observer

Appendix C:

Background on The Sedona Conference℠ and its Working Group Series

Executive Director
Richard G. Braman, Esq.

180 Broken Arrow Way So.
Sedona, Arizona 86351
Ph: Toll Free 1-866-860-6600
Fx: 928-284-4240
Email: tsc@sedona.net
www.thesedonaconference.org

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. We meet 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, we host four conferences a 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 40 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 Conference has received broad and strong accolades from participants since its inception (see "Raves" portion 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. The conferences in the Working Group Series begin with the same high caliber of participants as our regular season faculty and attendees. The total group, however, is limited to 30 or so. Further, in lieu of finished papers being posted on our website in advance of the conference, thought pieces and other ideas and background information are exchanged ahead of time, and the conference itself becomes the opportunity to create a set of recommendations, guidelines or other position piece. Working Group output will then be put through a peer review process, including critique at one of our regular season conferences, before revision and republication.

Through a combination of our new Working Group Series and regular season conferences we hope to be able to develop peer-reviewed, authoritative sets of principles, or guidelines, on difficult issues confronted daily by participants in our legal system. Future Working Groups are currently under consideration in two areas: (1)protective orders, secrecy and the public interest; (2) guidelines on professionalism and bench-bar relations in an effort to help avoid the increasing isolation of our judiciary; and (3) patents, innovation and litigation. Please contact us by email at tsc@sedona.net if you are interested in learning more about our Working Groups or their output. Further information about The Sedona Conference℠ and our Working Group Series is also available on our website: www.thesedonaconference.org.

Visit www.thesedonaconference.org