The Sedona Conference® Working Group Series

WGS℠

The Sedona Principles:
Second Edition
Best Practices Recommendations & Principles for Addressing Electronic Document Production

A Project of The Sedona Conference®
Working Group on Electronic Document
Retention & Production (WG1)

June 2007

The Sedona Conference®

The Sedona Principles
(Second Edition)
Addressing Electronic Document Production

Editor in Chief: Jonathan M. Redgrave

Executive Editors:
Richard G. Braman
Kenneth J. Withers

Senior Editors:
Thomas Y. Allman
Conor R. Crowley
Ted S. Hiser

Technology Advisor: John H. Jessen

REPRINT REQUESTS:
Requests for reprints or reprint information should be directed to
Richard Braman, Executive Director of The Sedona Conference,
at tsc@sedona.net or 1-866-860-6600.

The editors wish to thank Jessica Buffenstein and David Degnan
for their tireless efforts cite-checking and proofreading.

Foreword

Welcome to the Second Edition of *The Sedona Principles: Best Practices Recommendations and Principles for Addressing Electronic Document Production*, a project of The Sedona Conference® Working Group on Best Practices for Electronic Document Retention and Production (WG1). The Sedona Conference® Working Group Series (WGS℠) 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 D for further information about The Sedona Conference® in general, and the WGS℠ in particular).

Since the first publication of *The Sedona Principles* in January 2004, the *2004 Annotated Version of The Sedona Principles* in the Spring of 2004, and the July 2005 version of *The Sedona Principles,* there have been many developments in the case law as well as significant amendments to the Federal Rules of Civil Procedure and several state civil procedure rules. The Principles, however, have maintained their vitality.

The Second Edition includes updates throughout the Principles and Comments reflecting the new language found in the amended Federal Rules and advances in both jurisprudence and technology. The Introduction has been expanded to include a comparison of *The Sedona Principles* with the amended Federal Rules. Particular attention has been given to updating the language and commentary on Principle 12 (metadata) and Principle 14 (the imposition of sanctions).

The Second Edition has also been rearranged for ease of reference. The 14 Principles themselves are found in the front of this publication, together with a chart cross-referencing each Principle to corresponding sections of the amended Federal Rules of Civil Procedure. In the body of this publication, each rule is followed by one or more Comments, most of which include a "Resources and Authorities" section pointing the reader to selected leading case law, exemplar court rules, and leading legal scholarship for further study.

This version also includes other clerical, minor stylistic, and grammatical edits, as well as updates of the appendices. Since The Sedona Conference® has now published *The Sedona Conference Glossary: E-Discovery and Digital Information Management,* we have eliminated the separate glossary that previously appeared as Appendix A to *The Sedona Principles.*

I want to thank the entire Working Group for all their hard work and contributions, and especially the Editorial Committee and Steering Committee for leading this effort to arrive at the new milestone of a Second Edition! Finally, but certainly not least, the Working Groups of The Sedona Conference could not accomplish their goals without the financial support of the sustaining and annual sponsors of the Working Group Series listed at www.thesedonaconference.org/sponsorship.

Richard G. Braman
Executive Director
The Sedona Conference®
June 2007

The Sedona Principles for Electronic Document Production
Second Edition

1. Electronically stored information is potentially discoverable under Fed. R. Civ. P. 34 or its state equivalents. Organizations must properly preserve electronically stored information that can reasonably be anticipated to be relevant to litigation.

2. When balancing the cost, burden, and need for electronically stored information, courts and parties should apply the proportionality standard embodied in Fed. R. Civ. P. 26(b)(2)(C) and its state equivalents, which require consideration of the technological feasibility and realistic costs of preserving, retrieving, reviewing, and producing electronically stored information, 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 electronically stored information when these matters are at issue in the litigation and seek to agree on the scope of each party's rights and responsibilities.

4. Discovery requests for electronically stored information should be as clear as possible, while responses and objections to discovery should disclose the scope and limits of the production.

5. The obligation to preserve electronically stored information 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 electronically stored information.

6. Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information.

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

8. The primary source of electronically stored information for production should be active data and information. Resort to disaster recovery backup tapes and other sources of electronically stored information that are not reasonably accessible requires the requesting party to demonstrate need and relevance that outweigh the costs and burdens of retrieving and processing the electronically stored information from such sources, including the disruption of business and information management activities.

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 electronically stored information.

10. A responding party should follow reasonable procedures to protect privileges and objections in connection with the production of electronically stored information.

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

12. Absent party agreement or court order specifying the form or forms of production, production should be made in the form or forms in which the information is ordinarily maintained or in a reasonably usable form, taking into account the need to produce reasonably accessible metadata that will enable the receiving party to have the same ability to access, search, and display the information as the producing party where appropriate or necessary in light of the nature of the information and the needs of the case.

13. Absent a specific objection, party agreement or court order, the reasonable costs of retrieving and reviewing electronically stored 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 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 may be shared by or shifted to the requesting party.

14. Sanctions, including spoliation findings, should be considered by the court only if it finds that there was a clear duty to preserve, a culpable failure to preserve and produce relevant electronically stored information, and a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.

The Sedona Principles & the Federal Rules

Topic of Discussion	Sedona Principle	Federal Rule(s) (amended 2006)	Relevant Sedona Comment(s)
Discovery Scope	Principles 1, 2, 5, 6, 8, 9, 11	Rule 34(a)	Comments 1a, 2a, 2b, 2c, 3a, 5a, 6c, 8a, 9a, 9b, 11a, 11b
Preservation Obligations	Principles 1, 3, 5, 6, 8, 9, 12	n.a.	Comments 1c, 2c, 3a, 3d, 5a, 5b, 5c, 5d, 5e, 5g, 5h, 5i, 6a, 6b, 6d, 6e, 6f, 8c, 9b, 12a, 12b, 14a
Form of Preservation	Principle 12	n.a.	Comments 12a, 12b
Metadata	Principle 12	n.a.	Comments 6f, 12a, 12b, 12c, 12d
Form of Production	Principles 4, 12	Rule 34(b)	Comments 3b, 4a, 12a, 12b, 12d
Meet and Confer	Principle 3	Rule 26(f)	Comments 1d, 2e, 3a, 3b, 3c, 3d, 4a, 4c, 5a, 7a, 9a, 10a, 12c
Initial Disclosure	Principle 3	Rule 26(a)(1)	Comment 3d
Preservation Orders	Principle 5	n.a.	Comment 5f
Discovery Requests	Principle 4	Rule 34(a)	Comment 3b, 4a, 4b
Tiered Production	Principle 8	Rule 26(b)(2)(B)	Comments 2c, 8a, 8b, 9a
Cost-Shifting	Principle 13	Rule 26(b)(2)(B)	Comments 2c, 13a, 13b, 13c
Proportionality Limits	Principle 2	Rule 26(b)(2)(C) (was Rule 26(b)(2)(b)	Comments 2a, 2b, 13b
ID of Unsearched Sources	Principle 4	Rule 26(b)(2)(B)	Comments 2c, 3a, 4b, 8b
Inadvertent Privilege Production	Principle 10	Rule 26(b)(2)(5)	Comments 10a, 10d
Spoliation Sanctions	Principle 14	n.a.	Comments 14a, 14b, 14c, 14d 14e, 14f
Safe Harbor	Principle 14	Rule 37(f)	Comments 14b, 14d, 14f
Nonparty Discovery	Principle 13	Rule 45	Comments 7b, 13c

Preface

On December 1, 2006, new rules took effect in federal courts governing the discovery of "electronically stored information" in civil litigation. The adoption of these rules represented a watershed in a process begun several years before, a process in which *The Sedona Principles* played a pivotal role. As judges and practitioners are being introduced to these new rules across the country, questions naturally arise as to the continued role of *The Sedona Principles* in e-discovery. Do the Federal Rules of Civil Procedure supplant *The Sedona Principles* as the primary source of guidance for judges, counsel, and clients facing electronic discovery? As important as the Federal Rules of Civil Procedure are, we believe the answer to that question is "no." The rules do not answer many of the most vexing questions judges and litigants face. They do not govern a litigant's conduct before suit is filed, nor do they provide substantive rules of law in such important areas as the duty of preservation or the waiver of attorney-client privilege. While the amended rules and the accompanying Committee Notes will be very influential references, they do not govern procedure in state court or in alternative dispute resolution forums. Far from supplanting *The Sedona Principles*, the new Federal Rules have highlighted the many areas of electronic discovery in which there is continued and growing need for guidance.

We have come a long way in five years. In the Spring of 2002, many of us who would later form the Sedona Conference® Working Group on Electronic Document Production began discussing ways to develop "best practices" for lawyers to follow in addressing electronic information in litigation and investigations. Litigants, particularly entities that generated large volumes of electronic information, did not know what obligations might apply to the preservation and production of electronic information. Clearly, the world was changing, and both the costs of discovery and risks of claims of evidence spoliation or discovery abuse threatened to rise. A cottage industry of electronic discovery consultants and continuing legal education providers was beginning to develop. Courts handled e-discovery disputes, but few decisions were reported and yet fewer provided meaningful guidance outside the context of particular facts. It seemed doubtful to us that the normal development of case law would yield, in a timely manner, the best practices for organizations to follow in producing electronic information.

In October 2002, The Sedona Conference® Working Group on Electronic Document Retention and Production, a group of attorneys and others experienced in electronic discovery matters, met to address the production of electronic information in discovery. The group was concerned about whether rules and concepts developed largely for paper discovery would be adequate to address issues of electronic discovery. After vigorous debate, a set of core principles emerged for addressing the production of electronic information. These principles became known as *The Sedona Principles*.

The initial draft was published in March of 2003 and widely disseminated by members of the Working Group and through the Internet and other channels. Between March and November of 2003, participants in the Working Group presented the draft *Sedona Principles* as part of more than twenty presentations to the bench and bar across the country. At these presentations, and in informal meetings and communications, participants solicited commentary and edits that could assist in revising the initial draft. Working Group participants also sought views from across the spectrum of the bar and consultants who are involved in this area.

The Working Group met again in October of 2003 to discuss and evaluate comments and possible revisions and to seek further input from Working Group members. The document was finalized in January 2004 and reflected the considered review of the initial draft and changes that were believed to enhance the document as a guide to courts, parties and counsel. A first "Annotated Version" was published in June 2004, the purpose being to show how the decisions of courts dovetailed or varied with *The Sedona Principles*. A 2005 Annotated Version was published in July 2005. By then, the case law on electronic discovery was burgeoning, as the references demonstrated. We now find that *The Sedona Principles* are at the center of a major evolution in how both federal and state courts treat electronic discovery, as is detailed in the Introduction. Accordingly, the commentary in this edition has been revised to include citations to other best practice guidelines and, in particular, to address the best practice guidelines in the context of the 2006 amendments to the Federal Rules of Civil Procedure concerning electronic discovery, effective December 1, 2006.

When the Working Group began its deliberations, the starting point was that under Rule 34 and many of its state counterparts, all "data compilations" were deemed documents just like traditional paper documents and subject to discovery. This equal treatment suggested that electronic information should be searched for, processed and produced like paper. However, the Working Group recognized that there are 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 electronic environments is inherently different from 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 have no paper analogue. The interpretation and application of the discovery rules had not accommodated these differences consistently and predictably so that litigants could efficiently and cost-effectively meet discovery obligations. The Working Group was conceived to help guide organizational practices and legal doctrine. In drafting the principles and commentary, we tried to keep in mind the "rule of reasonableness." That rule is embodied in Rule 1 of the Federal Rules of Civil Procedure (courts should secure the just, speedy and inexpensive determination of all matters) and is applied through former Rule 26(b)(2) (now renumbered as Rule 26(b)(2)(C) – proportionality test of burden, cost and need) and in many state counterparts. The rule of reasonableness means that litigants should seek – and the courts should permit – discovery that is reasonable and appropriate to the dispute at hand while not imposing excessive burdens and costs on litigants and the court. In addition, the Working Group operated on the premise that electronic information production standards could bring needed predictability to litigants and guidance to courts.

The Working Group unanimously concluded that dialogue between and among litigants was a prerequisite to resolving (or avoiding) potentially costly and disruptive electronic discovery disputes. We recognized that adversarial litigation, at times aggressively pursued, may make reasonable dialogue counter-intuitive. Nevertheless, the Working Group urged that parties were well-served by an early discussion about the issues in dispute, the types of information sought, the likely sources and locations of such information, and the realistic costs of identifying, locating, retrieving, reviewing, and producing such information. 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 to act in good faith also extends to the efforts taken to reasonably preserve relevant electronic information, to the form of the production, and to the allocation of the costs of the preservation and production. All discovery issues should be considered in light of the nature of the litigation and the amount in controversy, as well as the cost, burden, and disruption to the parties' operations.

The principles set forth herein were intended to be concrete enough to provide direction, but flexible enough to allow courts to fashion solutions for the inevitable exceptions. Indeed, the accompanying commentary reflects numerous circumstances and illustrations where the presumptive rule must be adapted to the particular facts. Importantly, the absence of qualifiers and caveats from the stated principles should not be interpreted as a disregard for such circumstances or the need for careful application of the principles by courts, parties and counsel.

The Sedona Principles were intended originally to complement the Federal Rules of Civil Procedure, as they provided only broad standards, by establishing guidelines specifically tailored to address the unique challenges posed by production of electronically stored information. The hope was that, by encouraging before-the-fact and consistent guidance, parties would prepare for meaningful electronic discovery and avoid costly and uncertain discovery disputes. In addition, the Working Group believed it was essential to provide an analytical framework of the substantive law so that courts and counsel could better grapple with the application of the principles in the real world. The Working Group went so far as to suggest in the Preface to the original publication that the principles might also serve as the basis for new federal rules, state rules, or local court rules regarding electronic information production. The original editors wrote: "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."

The Advisory Committee on the Federal Rules of Civil Procedure met and published for public comment a set of draft amendments to the Federal Rules, specifically addressing electronic information, in August 2004. In the following six months, the Committee held three public hearings, heard oral testimony from 74 witnesses, and received 180 written submissions. In May 2005, revised proposals were sent to the Standing Committee on Rules of Practice and Procedure, and in September 2005 the Judicial Conference of the United States recommended that the U.S. Supreme Court adopt amendments to the Federal Rules of Civil Procedure specifically and substantially dealing with issues of what the Advisory Committee now dubbed "electronically stored information." In April 2006, the U.S. Supreme Court adopted the proposals, which ultimately became effective on December 1, 2006.

The Rules amendments adopt the concept that economies will be achieved if parties are required to meet as early as practicable to discuss issues surrounding discovery of electronically stored information. For the first time ever, the new Rules mention the duty to preserve information potentially relevant to litigation. The Rules also recognize that some electronically stored information may be difficult to access and produce, and establish a framework for identifying and evaluating whether the costs and burdens of producing some information outweigh the potential benefit to the resolution

of the dispute. Other amendments are also made with respect to the form of production, interrogatories, third party subpoenas, inadvertent production of privileged documents, and, to a limited extent, grounds for imposing sanctions.

Meanwhile, the Working Group has continued to meet, and publish, on topics relevant to how to handle electronic information in the context of litigation or investigations. The small group of twenty-four that first met in October 2002 has now grown to more than 400, with participation from the bench, academia, government, and all segments of the civil bar.

This publication, like the original *Sedona Principles*, has three major components. It starts by setting forth the 14 Sedona Principles, followed by a chart cross-referencing *The Sedona Principles* with the amended Federal Rules of Civil Procedure. An Introduction sets forth the basic concepts of electronic discovery and summarizes the role of *The Sedona Principles* in both federal and state courts. The following section sets forth the 14 Sedona Principles. These principles embody the consensus views of the Working Group participants and represent what we believe is a reasonable and balanced approach to the treatment of electronic data. The third component, detailed commentary, expands the basic formulations of the principles into a more comprehensive analysis to address the presumptions, legal doctrines, and certain notable exceptions to the application of the principles. These detailed Comments, divided into logical groupings, are supported by select citations to leading cases and references to key secondary sources and authorities, including the Conference of Chief Justices' Guidelines and other recent scholarship. Throughout, the document has been updated to take into account the 2006 Amendments to the Federal Rules, and also to discuss the numerous important court decisions that are influencing the development of the law in this area. Particular attention has been paid to updating Principle 12 on the preservation and production of metadata and Principle 14 on the imposition of sanctions.

Working Group 1 Steering Committee:

Thomas Y. Allman
Conor R. Crowley
Sherry B. Harris
John H. Jessen
Timothy L. Moorehead
Ashish S. Prasad
Jonathan M. Redgrave
Ariana J. Tadler
Lori Ann Wagner[1]

June 2007

[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®, any one participant (or observer) or law firm/company employing a participant or any of their clients. A list of all participants and members of the Working Group (as well as observers to the process) is set forth in Appendix C.

Table of Contents

Table of Contents, cont.

Table of Contents, cont.

Table of Contents, cont.

Table of Contents, cont.

Introduction

Discovery in a World of Electronically Stored Information

Discovery, and document production in particular, is a familiar aspect of litigation practice for many lawyers. The explosive growth and diversification of electronic methods for recording, communicating, and managing information has transformed the meaning of the term "document." While twenty years ago PCs were a novelty and email was virtually nonexistent, today more than ninety percent of all information is created in an electronic format.

For courts and lawyers, whose practices are steeped in tradition and precedent, the pace of technological and business change presents a particular challenge.[2] As electronically stored information (often referred to as "ESI") has become more prevalent, courts, litigants, and rule-makers have attempted to meet this challenge, sometimes by applying traditional approaches to discovery, sometimes by turning to treatises (including earlier editions of *The Sedona Principles*), and sometimes by innovating.

Civil litigation in the federal courts is governed by the Federal Rules of Civil Procedure, which were amended in 2006 to include explicit, and in some cases, unique provisions to govern the discovery of electronically stored information.[3] In the main, the Federal Rules are consistent with and reflect the same approach as *The Sedona Principles*. However, there are differences that are discussed in more detail below.

This revised edition of *The Sedona Principles* seeks to synthesize the current and best thinking from the case law and the amended Federal Rules to provide practical standards for modern discovery.[4]

1. What Is Electronic Discovery?

Electronic discovery refers to the discovery of electronically stored information. Electronically stored information includes email, web pages, word processing files, audio and video files, images, computer databases, and virtually anything that is stored on a computing device – including but not limited to servers, desktops, laptops, cell phones, hard drives, flash drives, PDAs and MP3 players. Technically, information is "electronic" if it exists in a medium that can only be read through the use of computers. Such media include cache memory, magnetic disks (such as computer hard drives or floppy disks), optical disks (such as DVDs or CDs), and magnetic tapes. Electronic discovery is often distinguished from "conventional" discovery, which refers to the discovery of information recorded on paper, film, or other media, which can be read without the aid of a computer. Of course, there is also the discovery of tangible "things" which usually refers to physical objects and property.

For readers less familiar with technical terms relevant to electronic discovery, a glossary of terms is provided in *The Sedona Conference Glossary: E-Discovery & Digital Information Management,* which is *available at* http://www.thesedonaconference.org.

---

2 "[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.'" Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice & Procedure,* § 2218 at 449 (2d ed. 2006) (quoting *Bills v. Kennecott Corp.,* 108 F.R.D. 459, 462 (D. Utah 1985)). Similarly, the *Manual for Complex Litigation* recognizes that the benefits and problems associated with computerized data are substantial in the discovery process. *Manual for Complex Litigation (Fourth)*, § 21.446 (Fed. Jud. Ctr. 2004).

3 The 2006 amendments to the Federal Rules of Civil Procedure addressing the discovery of electronically stored information became effective December 1, 2006. *See* http://www.uscourts.gov/rules.gov/rules/EDiscovery_w_Notes.pdf. The amendments impact rules 16, 26, 33, 34, 37, 45 and Form 35. For a summary of the new rules and competing viewpoints on their efficacy, see Thomas Y. Allman, *The Impact of the Proposed Federal E-Discovery Rules,* 12 Rich. L. J. & Tech. 13 (2006); Richard L. Marcus, *E-Discovery & Beyond: Toward Brave New World or 1984?* 236 F.R.D. 598, 618 (2006) and Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure,* 4 Nw. J. Tech. & Intell. Prop. 171 (2006), *available at* http://www.northwestern.edu/journals/njtip/v4/n2/3. Unless otherwise indicated, all references to the Federal Rules of Civil Procedure and accompanying Committee Notes are to the language in force December 1, 2006. Shortly after completion of the amendments addressing electronic discovery, the entire Federal Rules of Civil Procedure underwent "restyling," a process intended to clarify and simplify the language and presentation of the rules without affecting their substantive meaning. *See* http://www.uscourts.gov/rules/supct1106/CV_CLEAN_FINAL5-30-07.pdf. The restyled rules are anticipated to go into effect December 1, 2007. While a full analysis of any effect the restyling may have on the interpretation or application of the rules remains for a future date, the Editors wish to point out that the restyling likely will result in one significant nonsubstantive change – Fed. R. Civ. P. 37(f) addressing sanctions for the failure to produce electronically stored information will be renumbered Fed. R. Civ. P. 37(e). See Principle 14, *infra*.

4 *See Zubulake v. UBS Warburg,* 229 F.R.D. 422, 440 (S.D.N.Y. 2004) (*"Zubulake V"*) (citing the ABA Standards and *The Sedona Principles,* in addition to the evolving revisions to the Federal Rules and local District Rules).

2. How is Discovery of Electronically Stored Information Different?

The answer to the question –"why and how is electronic discovery different?" – lies in the subtle, but sometimes profound, ways in which electronically stored information presents unique opportunities and problems for document production. Magistrate Judge Nan Nolan noted some of these differences in *Byers v. Illinois State Police*, 53 Fed. R. Serv. 3d 740, No. 99 C 8105, 2002 WL 1264004 (N.D. Ill. May 31, 2002):

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

Id. at *31-33.

The qualitative and quantitative differences between producing paper documents and electronic information can be grouped into the following six broad categories.

A. Volume and Duplicability

There is substantially more electronically stored information than paper documents, and electronically stored information is created and replicated at much greater rates than paper documents.

The dramatic increase in email usage and electronic file generation poses particular problems for large data producers, both public and private. A single large entity can generate and receive millions of emails and electronic files each day. A very high percentage of information essential to the operation of public and private enterprises is stored in electronic format and much is never printed to paper. Not surprisingly, the proliferation of the use of electronically stored information has resulted in vast information 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.

Electronic information is subject to rapid and large scale user-created and automated replication without degradation of the data. Email provides a good example. Email users frequently send the same email to many recipients. These recipients, in turn, often forward the message, and so on. At the same time, email software and the systems used to transmit the messages automatically create multiple copies as the messages are sent and resent. Similarly, other business applications are designed to periodically and automatically make copies of data. Examples of these include web pages that are automatically saved as cache files and file data that is routinely backed up to protect against inadvertent deletion or system failure.[5]

---

[5] Neither the users who created the data nor information technology personnel are necessarily aware of the existence and locations of the 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 email, on a backup tape, in an internet cache, and on portable media such as a CD or floppy disk. Furthermore, the location of particular electronic files typically is determined not by their substantive content, but by the software with which they were created, making organized retention and review of those documents difficult.

B. Persistence

Electronically stored information is more difficult to dispose of than paper documents. A shredded paper document is essentially irretrievable.[6] Likewise, a paper document that has been discarded and taken off the premises for disposal as trash is generally considered to be beyond recovery. Disposal of electronically stored information is another matter altogether. The term "deleted" is misleading in the context of electronic data, because it does not equate to "destroyed." Ordinarily, "deleting" a file does not actually erase the data from the computer's storage devices. Rather, it simply finds the data's entry in the disk directory and changes it to a "not used" status – thus permitting the computer to write over the "deleted" data. Until the computer writes over the "deleted" data, however, it may be recovered by searching the disk itself rather than the disk's directory. This persistence of electronic data compounds the rate at which electronic data accumulates and creates an entire subset of electronically stored information that exists unknown to most individuals with custody and ostensible control over it.

C. Dynamic, Changeable Content

Computer information, unlike paper, has content that is designed to change over time even without human intervention. Examples include: workflow systems that automatically update files and transfer data from one location to another; backup applications that move data from one storage area to another to function properly; web pages that are constantly updated with information fed from other applications; and email systems that reorganize and purge data automatically. As a result, unlike paper documents, much electronically stored information is not fixed in a final form.

More generally, electronically stored information is more easily and more thoroughly changeable than paper documents. Electronically stored information 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 may alter data contained on it. Simply moving a word processing file from one location to another may change creation or modification dates found in the metadata. In addition, earlier drafts of documents may be retained without the user's knowledge.

D. Metadata

A large amount of electronically stored information, unlike paper, is associated with or contains information that is not readily apparent on the screen view of the file. This additional information is usually known as "metadata." Metadata includes information about the document or file that is recorded by the computer to assist in storing and retrieving the document or file. The information may also be useful for system administration as it reflects data regarding the generation, handling, transfer, and storage of the document or file within the computer system. Much metadata is neither created by nor normally accessible to the computer user.

There are many examples of metadata. Such information includes file designation, create and edit dates, authorship, comments, and edit history. Indeed, electronic files may contain hundreds or even thousands of pieces of such information. For instance, email has its own metadata elements that include, among about 1,200 or more properties, such information as the dates that mail was sent, received, replied to or forwarded, blind carbon copy ("bcc") information, and sender address book information. Typical word processing documents not only include prior changes and edits but also hidden codes that determine such features as paragraphing, font, and line spacing. The ability to recall inadvertently deleted information is another familiar function, as is tracking of creation and modification dates.

---

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

Similarly, electronically created spreadsheets may contain calculations that are not visible in a printed version or hidden columns that can only be viewed by accessing the spreadsheet in its "native" application, that is, the software application used to create or record the information. Internet documents contain hidden data that allow for the transmission of information between an internet user's computer and the server on which the internet document is located. So-called "meta-tags" allow search engines to locate websites responsive to specified search criteria. "Cookies" are text files placed on a computer (sometimes without user knowledge) that can, among other things, track usage and transmit information back to the cookie's originator.[7]

Generally, the metadata associated with files used by most people today (such as Microsoft Office™ documents) is known as "application metadata." This metadata is embedded in the file it describes and moves with the file when it is moved or copied. On the other hand, "system metadata" is not embedded within the file it describes but stored externally. System metadata is used by the computer's file system to track file locations and store information about each file's name, size, creation, modification, and usage.

Understanding when metadata is relevant and needs to be preserved and produced represents one of the biggest challenges in electronic discovery. Sometimes metadata is needed to authenticate a disputed document or to establish facts material to a dispute, such as when a file was accessed in a suit involving theft of trade secrets. In most cases, however, the metadata will have no material evidentiary value – it does not matter when a document was printed, or who typed the revisions, or what edits were made before the document was circulated. There is also the real danger that information recorded by the computer as application metadata may be inaccurate. For example, when a new employee uses a word processing program to create a memorandum by using a memorandum template created by a former employee, the metadata for the new memorandum may incorrectly identify the former employee as the author. However, the proper use of metadata in litigation may be able to provide substantial benefit by facilitating more effective and efficient searching and retrieval of electronically stored information.

E. Environment-Dependence and Obsolescence

Electronic data, unlike paper data, may be incomprehensible when separated from its environment.[8] For example, the information in a database may be incomprehensible when removed from the structure in which it was created. If the raw data (without the underlying structure) in a database is produced, it will appear as merely a long list of undefined numbers. To make sense of the data, a viewer needs the context, including labels, columns, report formats, and similar information. Report formats, in particular, allow understandable, useable information to be produced without producing the entire database. Similarly, stripping metadata and embedded data from data files such as spreadsheets can substantially impair the functionality of the file and the accuracy of the production as a fair representation of the file as kept and used in the ordinary course of business.

Also, it is not unusual for an organization to undergo several migrations of data to different platforms within a few years. Because of rapid changes in computer technology, neither the personnel familiar with the obsolete systems nor the technological infrastructure necessary to restore the out-of-date systems may be available when this "legacy" data needs to be accessed. In a perfect world, electronically stored information that has continuing value for business purposes or litigation would be converted for use in successor systems, and all other data would be discarded. In reality, such migrations are rarely flawless.

---

7 There is much confusion over the use of terms and distinctions between application and systems metadata can be confusing. *See* Craig Ball, *Understanding Metadata: Knowing Metadata's Different Forms and Evidentiary Significance Is Now an Essential Skill for Litigators,* 13 Law Tech. Prod. News 36 (Jan. 2006).

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

F. Dispersion and Searchability

While a user's paper documents will often be consolidated in a handful of boxes or filing cabinets, the user's electronically stored information may reside in numerous locations – desktop hard drives, laptop computers, network servers, floppy disks, flash drives, CD-ROMS, DVDs and backup tapes. Many of these electronic documents may be identical backup or archive copies. However, some documents may be earlier versions drafted by that user or by other users who can access those documents through a shared electronic environment.

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

While the dispersed nature of electronically stored information complicates discovery, the fact that many forms of electronically stored information and media can be searched quickly and accurately by automated methods provides new efficiencies and economies. In many instances, software is able to search far greater volumes of these types of electronically stored information than human beings could review manually.

3. What Are *The Sedona Principles* and How Have They Influenced the Evolution of E-Discovery?

The reliance upon discovery of electronically stored information has increased markedly in the last decade, although indications of its growing importance to civil litigation have been apparent since the early 1980s.

The Sedona Principles are at the heart of two major parallel developments, one involving the identification and articulation of "best practices" and the other involving rulemaking. The *Principles* evolved from discussions involving wide segments of the parties affected by and deeply involved in the actual e-discovery practice and represent a consensus viewpoint. They evolved into "final" form by 2004. The focus on best-practice guidelines is also embodied in the American Bar Association's "Civil Discovery Standards" and the Conference of Chief Justices' "Guidelines for State Trial Courts." On the rulemaking front, early developments at the state level[9] were followed by the work of the Advisory Committee on Civil Rules of the Judicial Conference of the United States, beginning in 2000, to explore the need for targeted rulemaking. That effort resulted in the 2006 amendments to the Federal Rules of Civil Procedure (the "amended Federal Rules" or the "2006 amendments"). Since the adoption of the amended Federal Rules, a number of states have begun to consider whether to adopt some form of e-discovery rules or guidelines. Many appear to be awaiting the consequences of the federal amendments. Other states require or encourage early discussions of preservation issues and identification of key sources of electronically stored information.[10] An effort by the Uniform Law Commissioners to promote uniform rulemaking modeled on the amended Federal Rules is also underway.

The Sedona Principles have an impressive track record of providing useful assistance to individual federal and state courts facing novel e-discovery issues. They have been influential in providing intellectual support in a number of precedent-

[9] The State of Texas was the first state to enact formal e-discovery rules, having added Rules §§196.3 and 196.4 to its Rules of Civil Procedure in 1999. The State of Mississippi enacted a similar rule in 2003.

[10] *See* New York Rules for the Commercial Division of the Supreme Court, §202.70(g).

setting cases involving preservation obligations,[11] search methodology,[12] production of metadata[13] and the handling of privileged information,[14] to name only a few examples.

We anticipate that the role of providing guidance and best practices will continue to be the province of *The Sedona Principles* – a process illustrated by the changes in Principles 12 (metadata) and 14 (sanctions), as well as the expanded commentary under all fourteen principles. Indeed, there are efforts underway to adopt similar principles in Canada and other countries.[15]

4. What is the Relationship Between *The Sedona Principles* and Court Rules?

A. Federal Rules of Civil Procedure

The Sedona Principles helped shape the legal environment in which the amended Federal Rules were drafted and adopted. In turn, the 2007 revision of *The Sedona Principles* is heavily influenced by consideration of the amended Federal Rules. This interplay between *The Sedona Principles* and the amended Federal Rules will continue. However, *The Sedona Principles* address a number of key topics that the amendments do not. For example, civil procedure rules only apply once litigation commences, and are procedural and not substantive. Therefore the amended Federal Rules do not establish standards governing pre-litigation preservation.[16] *The Sedona Principles* cover the topic in several best practice standards which continue to play a major role in the developing national consensus on the topic.[17]

In many respects, the processes and procedures adopted in the amended Federal Rules and *The Sedona Principles* are consistent. A summary chart comparing *The Sedona Principles* and the amended Federal Rules, by key topics, is found in the front of this publication.

(i) Scope of Discovery of Electronically Stored Information. Amended Federal Rule 34 now provides for the discovery[18] of "electronically stored information" as well as documents and tangible things. This clarification of the scope of discovery parallels Sedona Principle 1 that electronic information of all forms and in all media is potentially subject to discovery. For consistency, the Working Group has adopted the phrase "electronically stored information" for use throughout *The Sedona Principles* in order to employ terminology that is consistent with the Rules.[19]

---

11 *Consolidated Aluminum Corp. v. Alcoa, Inc.*, No. 03-1055-C-M2, 2006 WL 2583308, at *6 n. 18 (M.D. La. July 19, 2006) (relying on *The Sedona Principles* in determining scope of preservation obligation).

12 *Treppel v. Biovail,* 233 F.R.D. 363 (S.D. N.Y. 2006) (relying on *The Sedona Principles* in determining appropriateness of defined search strategies required).

13 *Williams v. Sprint/United Management Co.*, 230 F.R.D. 640 (D. Kan. 2005) (relying on *The Sedona Principles* in determining whether production of metadata was required).

14 *Hopson v. The Mayor and City Council of Baltimore,* 232 F.R.D. 228, 234 (D. Md. 2005) (relying on *The Sedona Principles* in establishing protocol for privileged document clawback agreement).

15 *See The Sedona Canada Principles* (A Project of The Sedona Conference Working Group 7 (WG7)) (February 2007 Public Comment Draft) *available at* http://www.thesedonaconference.org.

16 Thomas Y. Allman, *Rule 37(f) Meets Its Critics: The Justification for A Limited Safe Harbor for ESI, 5* Nw. J. Tech. & Intell. Prop. 1 (2006).

17 *See* Sedona Principle 5 (a party must act reasonably and in good faith in executing preservation obligations, but is not expected to take every conceivable step). Other principles dealing with preservation obligations are Principle 3 (early discussion); 6 (presumptions regarding responding parties); 8 (disaster recovery backup tapes); 9 (deleted, shadowed, fragments or residual data); 12 (metadata) and 14 (sanctions for failure to preserve).

18 Fed. R. Civ. P. 26(a)(1), which requires "initial disclosures" independent of the Rule 34 discovery request process, also includes an obligation to disclose electronically stored information which a party intends to use to support its claims or defenses.

19 Even before "electronically stored information" was explicitly added to Rule 34, it was "black-letter law that computerized data is discoverable if relevant." *Anti-Monopoly, Inc. v. Hasbro, Inc.*, No. 94 Civ. 2120, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995); *see also Bills v. Kennecott Corp.*, 108 F.R.D. 459, 463-64 (D. Utah 1985) ("[I]nformation stored in computers should be as freely discoverable as information not stored in computers.").

(ii) Limits on Required Production (General). All discovery – including discovery of electronically stored information – is subject to the proportionality limits set forth in Rule 26(b)(2)(C), which require a court to weigh the potential benefit or importance of requested information against the burden on the party that would have to produce the documents.[20] Rule 26(b)(2)(C)(iii) provides for limiting discovery when "the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues." Rule 26(b)(2)(C)(i) provides that discovery may be limited if "the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive." The Federal Rules are intended to protect parties from unduly burdensome, unnecessary, or inefficient discovery. Rule 26(b)(1) limits discovery to matters, not privileged, which are relevant to a claim or defense.

The Sedona Principles reflect these limits in Principle 2, which provides that "the technological feasibility and realistic costs of preserving, retrieving, reviewing, and producing electronically stored information" should be taken into account in achieving balance. Principle 6 acknowledges and expands the concept by noting that "responding parties are best situated" to evaluate the appropriate procedures, methodologies and technologies to preserve and produce their electronically stored information.

(iii) Limits on Discovery Based on Accessibility. Rule 26(b)(2)(B) establishes a two-tiered approach to discovery unique to the production of electronically stored information. Relevant electronically stored information that resides on sources that are identified as "not reasonably accessible because of undue burden or cost" may be withheld from production, without resort to a court order, provided there is an appropriate identification of the sources of electronically stored information that are not being produced. If the producing party can sustain the burden of demonstrating the undue burden or costs on a challenge, the requesting party then has the burden to show "good cause" for production from these sources.[21] Cost-shifting may be ordered as a condition of production.

Sedona Principle 8 also suggests an initial presumptive limit on discovery, but relates the limit on the initial scope of discovery for relevant evidence to the actual use of information in a business. Sedona Principle 8 states that the "primary source" for discovery should be "active data and information." The commentary to Principle 8 harmonizes the two approaches.

(iv) Protective Orders and Cost-Shifting. Rule 26(c) allows a court to enter a protective order against burdensome discovery and historically is the source of the authority to shift costs for all forms of discovery. The 2006 amendments reinforce this by adding a provision in Rule 26(b)(2)(B) that a producing party may seek a protective order to test its obligations to preserve or produce electronically stored information.

Unlike the Federal Rules, Sedona Principle 13 explicitly states that the costs of "retrieving and reviewing" electronically stored information that is not "reasonably available" may be shifted to the requesting party. The revised commentary under Principle 13 addresses the differences, as well as distinction, between cost shifting under Rule 26(b)(2)(B) and Rule 26(c).

---

20 *See In re Microcrystalline Cellulose Antitrust Litig.*, 221 F.R.D. 428, 429 (E.D. Pa. 2004) (applying limits of Rule 26 (b)(2) (prior to renumbering) to limit unreasonable demand for sales data not needed in antitrust action).

21 Ordinarily a requesting party should obtain and evaluate the information from accessible sources before insisting that the responding party search and produce from sources that are not reasonably accessible. *See* Fed. R. Civ. P. 26(b) Committee Note.

(v) Mandatory Early Discussions. The Rule 26(f) requirement for an early "meet and confer" prior to the Rule 16 scheduling conference has been substantially strengthened and expanded in a manner similar to that advocated by Sedona Principle 3.[22] Parties are now expected to have early and meaningful discussions of "any issues relating to preserving discoverable information" and to develop a proposed discovery plan that takes into account "disclosure or discovery" of electronically stored information including, but not limited to, both the form of production and the method of handling claims of privilege after production.

(vi) Form of Production and Metadata. Electronically stored information is created in a form "native" to that application and computer system, together with system and application metadata. This electronically stored information may be produced in a variety of forms other than its "native" form. Some forms of production replicate the view of the user and provide other capabilities such as searchability, but with limited or no metadata or embedded data. The Advisory Committee rejected proposals to mandate any particular form of production and did not take a position on the need to produce metadata. Rule 26(f) instead emphasizes the need to discuss this topic early to attempt to reach agreement, and Rule 34(b) provides a process for resolving disputes, while providing two alternative forms of production in the event the parties do not reach agreement or a court order is not entered: the form or forms "in which it is ordinarily maintained" or "in a form or forms that are reasonably usable."

The phrase "ordinarily maintained" is not synonymous with "native format." It is common for electronic information to be migrated to a number of different applications and formats in the ordinary course of business, particularly if the information is archived for long-term storage. Routine migration will likely result in the loss or alteration of some elements of metadata associated with the native application, and the addition of new elements. Given the variety of forms in which electronically stored information is found and the many options available in producing it, a difference may exist between the form in which electronically stored information is preserved and that in which it is produced for use, depending upon the issues involved and the preferences of the parties or any agreements or orders pending production.[23]

Sedona Principle 12, in contrast, deals directly with the issue of the need to preserve and produce metadata. It has been amended in this 2007 Version to provide more explicit guidance regarding issues relating to both the relevance and usability of metadata. Previously, Principle 12 only provided guidance on a narrow aspect of the metadata issue.[24]

(vii) Inadvertent Production of Privileged or Work Product Information. Because of the tremendous volume of electronically stored information that may need to be reviewed in response to a discovery request, and the complex nature of the information itself, which may contain metadata, embedded data, and non-obvious contextual links, reviewing electronically stored information for privilege is particularly difficult. Even the most diligent review is likely to result in some inadvertent production of privileged information. Serious practical and ethical issues exist when privileged information is inadvertently produced during discovery, not the least of which is the potential waiver under applicable law.[25] Because rules of procedure cannot enlarge or abridge substantive rights, including the substantive law of privilege and waiver, the amended Federal Rules only create a procedure by which parties are now required, by Rule 26(f), to conduct an early discussion of the possible

---

22 *See* Sedona Principle 3, which states: "Parties should confer early in discovery regarding the preservation and production of electronic data and documents when these matters are at issue in the litigation, and seek to agree on the scope of each party's rights and responsibilities." Mandatory early discussion of contentious e-discovery issues was enthusiastically endorsed by many who testified at the Public Hearings in early 2005. The Testimony and filed Comments of almost 200 witnesses are accessible from the U.S. Courts website ("Comments"). *See* 2004 Civil Rules Committee Chart, including Request to Testify, *available at* http://www.uscourts.gov/rules/e-discovery.html. The Comments represent a valuable snapshot of e-discovery concerns and practices as of 2005 and contain many insightful observations.

23 *See In re Priceline.Com Inc. Securities Litig.*, 233 F.R.D. 88, 89-91 (D. Conn. 2005) (resolving disputes over the form of preservation and production by ordering that production be in TIFF and PDF form but that the original data be maintained in its original native file format for the duration of the litigation).

24 Sedona Principle 12 formerly focused on the need for the test of materiality in determining if preservation and production of metadata was needed. As implied in the *Priceline.Com* opinion, *supra*, it may be advisable to distinguish between the file format used in preservation and the form or forms used for production.

25 Jonathan M. Redgrave and Kristin M. Nimsger, *Electronic Discovery and Inadvertent Productions of Privileged Documents,* 49 Fed. Law. 37 (July 2002).

need for voluntary agreements to govern the treatment of a post-production privilege claim. Any agreement on the topic may be included in the Rule 16(b) Scheduling Order, but the Committee Notes recognize that such agreements between the parties, even if embodied in a court order, may not bind non-parties, a controversial subject being addressed by the Advisory Committee on the Rules of Evidence.[26] Rule 26(b)(5)(C) provides a standard procedure by which parties can identify and retrieve inadvertently produced documents and electronically stored information. It also sets forth a procedure by which the receiving party can challenge the privilege assertion.

Sedona Principle 10 is consistent with this approach, emphasizing the need for reasonable, mutually agreed-upon procedures to protect privileges and objections to production. Importantly, revisions to comment 10.d help to define and distinguish two common categories of agreements, the "clawback" and the "quick peek."

(viii) Sanction Limitations. The 2006 amendments do not directly address the nature and extent of preservation obligations. Instead, new Rule 37(f) limits the availability of rule-based sanctions when electronically stored information has been "lost as a result of the routine, good faith operation of an electronic information system."

While Rule 37(f) does not purport to limit the power to issue sanctions under a court's inherent power, this provision represents a considered policy decision intended to prevent unreasonable and unnecessary interruption of routine information systems during discovery.[27] *The Sedona Principles* do not include a directly comparable provision to Rule 37(f). Instead, Sedona Principle 14 focuses on the underlying issue – the elements required to justify the imposition of sanctions. The nature and extent of preservation obligations are discussed in general respects in Principles 1 and 5, with specific examples of how they apply in Principles 6, 7, 8, 9, 11 and 12.

A slight change in Principle 14 has been made in the 2007 version to more closely conform the culpability element in Principle 14 to emerging case law and to reflect the influence of the policy decision underlying Rule 37(f).[28]

(ix) Third Party Discovery. The obligations and protections added by the 2006 amendments generally apply to discovery of third parties. *See* Fed. R. Civ. P. 45. *The Sedona Principles* do not expressly distinguish between discovery of parties and non-parties, although the commentary does reflect the different treatment of non-parties versus parties in terms of evaluating burdens.

B. State Rules

The volume of reported e-discovery decisions has been smaller in state courts, leading to the misperception that electronic discovery was more prevalent in the types of disputes brought into federal court. As recently as a few years ago, outside the hotly contested areas of divorce law and employment disputes, few reported state court decisions existed. This is quickly changing as electronic discovery becomes more commonplace in state court litigation. *The Sedona Principles* have played a major role in these early cases.[29]

---

26 Proposed Evidence Rule 502, currently under consideration by the Advisory Committee Evidence Rules, addresses the impact on third parties of non-waiver agreements approved by the courts, among other topics. The proposed rule was approved by the Advisory Committee on Evidence on April 13, 2007, *available at* http://www.uscourts.gov/rules/Excerpt_EV_Report_Pub.pdf#page=4 .

27 *Turner v. Resort Condos. Int'l LLC*, No. 1:03-cv-2025, 2006 WL 1990379, at *8 (S.D. Ind. July 13, 2006) (refusing to issue sanctions for alleged failures in preservation where there was no bad faith alteration or destruction of evidence).

28 The clarification has been made that "grossly negligent" conduct can support sanctions for inadequate conduct in searching for discoverable information. *See Phoenix Four, Inc. v. Strategic Resources Corp.*, No. 05 Civ. 4837(HB), 2006 WL 1409413, at *9 (S.D.N.Y. May 23, 2006) (sanctioning party and counsel for failure to adequately search former servers used by defendant).

29 *See Bank of America Corp. v. SR Int'l Bus. Ins. Co.*, No. 05-CVS-5564, 2006 WL 3093174 (N.C. Super. Ct. Nov. 1, 2006).

It is by no means certain that the 2006 amendments to the Federal Rules will be adopted in the majority of the states. Rules of civil procedure are promulgated by the highest court in each state, based on input from committees or, in some cases, by action (or inaction) of legislative bodies.[30] Historically, while amendments to the Federal Rules of Civil Procedure have been highly influential on state procedural rulemaking, in recent years the benefits of uniformity have been questioned.[31] To some extent, this can be attributed to the frequency of changes in the rules and some unpopular experimentation, including the addition of mandatory disclosures in the 1993 rule amendments, modified in the 2000 amendments.

Two national initiatives are directed at promoting uniformity among the state trial courts. Both have been heavily influenced by *The Sedona Principles.* The first effort, which eschews formal rulemaking, is that of the Conference of Chief Justices ("CCJ") which has issued "Guidelines for State Trial Courts on Discovery of Electronically Stored Information" (August, 2006) (the "Guidelines").[32] The avowed purpose of the Guidelines is to provide "a reference document to assist state courts in considering issues related to electronic discovery," but not to supplant the rulemaking process of individual states ("[t]he Guidelines should not be treated as model rules that can simply be plugged into a state's procedural scheme"). The effort may be leading to some success at the state level.[33]

The second effort is that of the Electronic Discovery Committee of the National Conference of Commissioners on Uniform Laws ("NCCUSL") to develop uniform model discovery rules for adoption in the states.[34] Although still in draft form as of this writing, the effort to date has been closely modeled on the federal amendments.

5. Why Do Courts and Litigants Need Sedona Best Practice Standards Tailored to E-Discovery?

With the advent of the 2006 amendments to the Federal Rules, the dramatic growth in case law, and the increased number of best-practice guidelines such as those authored by the Conference of Chief Justices and the National Uniform Law Commissioners, it is fair to ask about the role remaining for best-practice standards like *The Sedona Principles*. The Federal Rules are necessarily procedural and cannot provide the level of detail found in *The Sedona Principles*.

Cases are necessarily fact specific. The Rules and Guidelines are not self-executing. A significant role likely remains for the evolution of current, authoritative best-practice standards and principles such as *The Sedona Principles* to provide guidance in the interpretation and application of electronic discovery rules and case law**.**

The Working Group began to examine the issue of electronic document production closely in 2002, focusing both on its similarities to and differences from paper document production. The principles and commentary that follow, as revised in 2007 Second Edition, reflect our continuing efforts to assist the reasoned and just evolution of the law as it relates to the preservation and production of electronically stored information.

---

30 *See* Linda S. Mullenix, *The Varieties of State Rulemaking Experience and the Consequences for Substantive Procedural Fairness* and *Table – State Rulemaking Authorities,* Roscoe Pound Institute 2005 Forum for State Appellate Court Judges, *available at* www.roscoepound.org/new/updates/2005Forum.htm.

31 *See* Stephen N. Subrin, *Federal Rules, Local Rules, and State Rules: Uniformity, Divergence, and Emerging Procedural Patterns,* 137 U. Pa. L. Rev. 1999 (1989) (movement leading to passage of Rules Enabling Act motivated in part by need for uniformity among courts prompted by the changes compelled by "the telephone, telegraph, train, and airplane").

32 The Conference of Chief Justices, *Guidelines for State Courts Regarding Discovery of Electronically Stored Information* (Aug. 2006), *available at* http://www.ncsconline.org/WC/Publications/CS_ElDiscCCJGuidelines.pdf.

33 *See Bank of America Corp., supra* note 29.

34 Information on the current status of the uniform model discovery rules is found at http://www.nccusl.org/Update/CommitteeSearchResults.aspx?committee=248.

Principles & Commentaries

1. Electronically stored information is potentially discoverable under Fed. R. Civ. P. 34 or its state equivalents. Organizations must properly preserve electronically stored information that can reasonably be anticipated to be relevant to litigation.

Comment 1.a. Discovery of electronically stored information under the 2006 Federal E-Discovery Amendments

Discovery in federal and state litigation extends to information relevant to the claims or defenses of a party or relevant to the subject matter of a dispute and likely to lead to the discovery of admissible evidence. This includes any machine-readable electronic information stored on physical media from which it can be retrieved, hereinafter referred to as "electronically stored information."

Before the 2006 amendments to Rule 34, there was some doubt in the federal courts about the full extent of discovery of some forms of electronic information due to Rule 34's focus on production of "documents." To some, the test of discoverability was synonymous with what was intentionally created or viewed by human users, and some doubt existed about other forms of electronic information, especially metadata and system information generated automatically by computers. Although Rule 34 was amended in 1970 to add "data compilations" to the list of discoverable documents, there was no suggestion that "data compilations" was intended to turn all forms of "data" into Rule 34 "documents."

Rule 34(a) has been clarified so that discovery extends to all stored information, including information that it is only readable by machine. Rule 34(a) states that discovery may be had of "electronically stored information (including writings, drawings, graphs, charts, photographs, sound recordings, images and other data or data compilations stored in any medium from which information can be obtained)." As with all discovery, of course, limits resting on the critical principle of proportionality are involved. *See* Principle 2, *infra.*

The form or forms in which the information should be produced, including the extent to which metadata should be produced, is a matter for early negotiation and discussion among parties. *See* Principle 12, *infra*. For cases governed by the Federal Rules, a procedure is set forth in Rule 34(b) to identify and discuss the form or forms of production of electronically stored information to be produced. Pending production, electronically stored information may be preserved in a variety of file formats, provided the relevant electronic content, and content searchability, are not degraded. *See also* Principles 9 and 12, *infra*. However, where special considerations are present, or the requesting party has so requested, consideration should be given to maintaining the information in its native format. *See* Principle 12, *infra*.

When electronically stored information is deleted, it is sometimes available as fragments, shadows, or residual portions of the original data set. This type of information is subject to discovery, but the evaluation of the need for and burdens of such discovery should be analyzed separately on a case-by-case basis. *See* Principle 9, *infra.*

The scope of discovery of electronically stored information does not depend on the internal designation or records classification that may or may not have been assigned to it. Any electronically stored information, whether or not it is internally viewed as of business, legal, regulatory, or personal value, is potentially discoverable.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 34(a).

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), *available at* http://www.uscourts.gov/rules/reports/st09-2005.pdf ("Advisory Committee Report").

Thomas Y. Allman, *The Impact of the Proposed Federal E-Discovery Rules,* 12 Rich. J.L. & Tech. 13 (2006).

Richard L. Marcus, *E-Discovery & Beyond: Toward Brave New World or 1984?* 236 F.R.D. 598, 618 (2006).

Lee H. Rosenthal, *A Few Thoughts on Electronic Discovery After December 1, 2006,* 116 Yale L.J. Pocket Part 167 (2006).

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 (2000).

Shira A. Scheindlin and Jonathan M. Redgrave, *Discovery of Electronic Information, in 2 Bus. and Commercial Litig. in Fed. Court,* Ch 22, (Robert L. Haig ed., 2005 and Supp. 2006).

Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure,* 4 Nw. J. of Tech. & Intell. Prop. 171 (2006), *available at* http://www.law.northwestern.edu/journals/njtip/v4/n2/3.

Comment, *Defining "Document" in the Digital Landscape of Electronic Discovery,* 38 Loy. L.A. L. Rev. 1541 (2005).

Panel Discussion, Advisory Committee Conference, Fordham University Law School, *Rule 33 and 34: Defining E-Documents and the Form of Production,* 73 Fordham L. Rev. 33 (2004).

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 324 (S.D.N.Y. 2003) (*"Zubulake I"*) (finding that plaintiff entitled to all emails and electronic documents relevant to employment discrimination claim, including those only preserved on backup tapes; however, given burden and expense of restoring inaccessible backup tapes, a cost-shifting analysis is appropriate).

Comment 1.b. The importance of proper records and information management policies and programs

Organizations should adopt policies and programs that provide rational and defensible guidelines for managing electronically stored information. These guidelines should be created after considering the business, regulatory, tax, information management, and infrastructure needs of the organization, including the need to conserve electronic storage space on email and other servers. Thus, a company that determines it only needs to retain email with business record significance should set forth such a practice in its document retention policy. Employees would then be responsible for implementing the policy, neither destroying documents and electronically stored information prematurely, nor retaining them beyond their useful life. Any such program should include provisions for legal holds to preserve documents and electronically stored information related to ongoing or reasonably anticipated litigation, governmental investigations, or audits. The existence, reasonableness and effectiveness in practice of such a program should be a significant consideration in any spoliation analysis.[35]

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

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

- establishing an appropriate and workable retention schedule for paper and electronically stored information
- helping business units establish practices and customs, tailored to the needs of their businesses, to identify the business records they need to retain
- addressing the retention of email and other communications, such as instant messaging and voicemail
- addressing other forms of electronically stored information that are created in the ordinary course of business
- developing communications policies that establish and promote the appropriate use of company systems. and
- training individuals to manage and retain business records created or received in the ordinary course of business.

Any records and information management program, regardless of its scope and provisions, should be accompanied by a "legal hold"[36] policy that applies once litigation or other investigatory demands are made known. *See* Principle 5, *infra*. These policies can assist in providing access to relevant material and help explain how the entity deals with preserving or collecting information subject to a hold.

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. 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.

A written records and information management policy can enable an organization to ensure that it is retaining all records necessary to the business, regulatory, and legal needs of the organization. A written policy can also provide guidance on how to properly dispose of documents, both written and electronic, that are without use to the organization. Such policies and programs allow an organization to demonstrate that it has legitimately destroyed documents and electronically stored information by following reasonable and objective standards. The United States Supreme Court noted that the existence of a reasonable records and information management policy, instituted and applied in good faith, should be considered in determining appropriate consequences for the destruction of evidence. *See Arthur Andersen LLP v. United States,* 544 U.S. 696 (2005).

Organizations should simultaneously address the retention and destruction of back-up media such that the storage and treatment of the information on such media are handled in a manner consistent with any records management or legal hold requirements. In some instances, an organization can address electronic and paper records and information with a single set of policies that require identical treatment. However, many entities find it necessary and appropriate to separate policies by functions and to employ technological resources for targeted and specific purposes.

---

[36] The nomenclature (e.g., "litigation hold") is not important; the important factor is that the organization has a means to comply with its legal obligations to preserve relevant information in the event of actual or reasonably anticipated litigation or investigation.

RESOURCES AND AUTHORITIES

The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information and Records in the Electronic Age, A Project of the Sedona Conference Working Group on Best Practices for Electronic Document Retention & Production (2007).

ANSI/ARMA Standard 9-2004, *Requirements for Managing Electronic Messages as Records,* ARMA International (Oct. 7, 2004).

Christopher R. Chase, *To Shred or Not to Shred: Document Retention Policies and Federal Obstruction of Justice Statutes,* 8 Fordham J. Corp. & Fin. L. 721 (2003).

Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005) ("'Document retention policies,' which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business … It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.").

Morris v. Union Pac. R.R. Co., 373 F.3d 896, 900 (8th Cir. 2004) (following Stevenson and distinguishing dicta in *Lewy v. Remington Arms Co.,* ruling that there must be a finding of intentional destruction indicating a desire to suppress the truth, and, in light of the trial court's conclusion that defendant did not intentionally destroy an audiotape of a collision, reversing and remanding for a new trial).

Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 751 (8th Cir. 2004) (defendant's routine document retention procecdure, which permitted it to destroy track maintenance records, was permissible before lawsuit commenced, but such records should have been preserved once litigation began).

Lewy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988) (establishing balancing test to determine appropriateness of adverse inference instruction and remanding for determination whether 1970 retention policy was reasonable considering the facts and circumstances of particular documents, and instituted in good faith; company may not blindly destroy documents).

Comment 1.c. Preservation in the context of litigation

An organization's document and information management policies and programs should focus on the business needs of the organization and the budgetary constraints on its use of technology. An organization also must retain documents and electronically stored information that may be relevant to current or reasonably anticipated litigation. *See* Principle 5 and associated commentary, *infra*. Further, most organizations are subject to statutory and regulatory constraints that require the preservation of particular documents and electronically stored information for specified time periods. 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.

Preservation obligations resemble the "retention" obligations imposed by business necessity, statutes, or regulations. However, while the retention schedules often focus on the "records" of an organization, the preservation duty goes further. For example, one of the typical subjects of discovery is unstructured information in the form of emails, word processing documents, spreadsheets, and the like, which may not be subject to the same retention schedules as formal "records." The duty to preserve may also extend, under some circumstances, to electronically stored information which takes the form of shadowed or residual data, which is embedded in a file, or is in sources deemed neither reasonably accessible nor part of the "records" managed by the entity. For all these reasons, care must be taken in designing and implementing processes to give notice of preservation obligations to appropriate custodians.

The duty to preserve transcends any requirements of internal policy or schedule regarding retention and destruction. As part of a legal hold process, a party should be prepared to take good faith measures to suspend or modify any feature of information systems which might impede the ability to preserve discoverable information.

The Federal Rules do not include specific articulations of the obligation to preserve electronically stored information, either with respect to the onset of the obligation, which is case specific, or its scope, which is influenced by the nature of the case and the types of potential claims and defenses involved. The precise preservation obligations must be determined on a case-by-case basis and will vary depending upon the types of electronically stored information involved. However, the 2006 Amendments, for the first time, acknowledged the intersection of preservation and procedure by amending Rule 26(f) to require discussion of "preservation" issues at the early "meet and confer" before the meeting with the court pursuant to Rule 16. In addition, Rule 37(f) was added to emphasize the role of procedures and processes in managing information systems and the risks involved in their "routine, good faith" operation. The Committee Notes make it clear that while preservation obligations arise independent of the Federal Rules, the good-faith obligation recognized in Rule 37(f) may require a party to take affirmative steps to prevent information systems from causing a loss of discoverable information.

Beyond satisfying these legal duties, however, it is neither feasible nor reasonable for organizations to take extraordinary measures to preserve documents and electronically stored information if there is no business or regulatory need to retain such documents and electronically stored information and there is no reasonable anticipation of litigation to which those documents may be relevant. For example, some commentators have observed that organizations should consider routinely making mirror image copies of employee disk drives when an employee leaves an organization or when computer equipment is recycled or discarded. While there may be unusual circumstances when that is advisable, as a general rule it would be wasteful and wholly unnecessary to accumulate such massive quantities of unused data because it is technically possible to do so. Rather, in accordance with existing records and information management principles, it is more rational to establish a procedure by which selected items of value can be identified and retained as necessary to meet the organization's legal and business needs when changes in personnel or hardware occur.

For a more detailed discussion of the preservation obligation as it applies to electronically stored information, see generally *Principle 5,* infra *and also Principles 2 (proportionality), 5 (general responsibility), 8 (disaster recovery backup tapes), 9 (deleted, shadowed, fragmented or residual information) and 12 (metadata).*

RESOURCES AND AUTHORITIES

Shira A. Scheindlin and Jonathan M. Redgrave, *Discovery of Electronic Information, in 2 Bus. & Commerical Litig. in Fed. Courts,* §§ 22:37 to 22:39 and 22:44 to 22:47 (Robert L. Haig ed., 2005 & Supp. 2006) (addressing duty to preserve, when the duty is imposed, and litigation hold procedures).

Ronald J. Hedges, *Discovery of Electronically Stored Information: Surveying the Legal Landscape,* Ch. III at 91-97 (BNA Books 2007) (addressing preservation issues).

Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005) ("'Document retention policies,' which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business …. It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.").

Morris v. Union Pac. R.R. Co., 373 F.3d 896, 900 (8th Cir. 2004) (following Stevenson and distinguishing dicta in *Lewy v. Remington Arms Co.,* ruling that there must be a finding of intentional destruction indicating a desire to suppress the truth, and, in light of the trial court's conclusion that defendant did not intentionally destroy an audiotape of a collision, reversing and remanding for a new trial).

Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 751 (8th Cir. 2004) (defendant's routine document retention procedure, which permitted it to destroy track maintenance records, was permissible before lawsuit commenced, but such records should have been preserved once litigation began).

Lewy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988) (establishing balancing test to determine appropriateness of adverse inference instruction and remanding for determination whether 1970 retention policy was reasonable considering the facts and circumstances of particular documents, and instituted in good faith; company may not blindly destroy documents).

Comment 1.d. Parties should be prepared to address records and information management policies and procedures at the initial meet and confer sessions

Amended Rule 26(f) requires early discussion of preservation issues and other disclosure and discovery issues involved in the production of electronically stored information. Because of the importance of existing records management policies and practices, it is likely that they will become the subject of discussion. Parties should be prepared to discuss, at least in general, their records management policies and practices, including the litigation hold process. In this regard, parties should consider when, and in what circumstances, a claim of privilege or attorney work product may be made with respect to litigation hold directives. In considering what information to discuss and what policies to produce, parties should consider the impact of production (or non-production) on any later need to demonstrate the good faith operation of records management programs and electronic information systems in the face of any claims of evidence spoliation. This and other topics relating to the early discussion at such conferences is supported by Principle 3. See discussion at Comments 3a and 3b, *infra*.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 26(f)(3) (requiring that parties discuss the discovery of electronically stored information at the initial meet and confer).

2. When balancing the cost, burden, and need for electronically stored information, courts and parties should apply the proportionality standard embodied in Fed. R. Civ. P. 26(b)(2)(C) and its state equivalents, which require consideration of the technological feasibility and realistic costs of preserving, retrieving, reviewing, and producing electronically stored information, as well as the nature of the litigation and the amount in controversy.

Comment 2.a. Scope of reasonable inquiry

The traditional approach to preserving and producing paper documents has been to undertake a good faith effort to identify sources and locations that are reasonably likely to contain relevant information and to advise custodians to preserve potentially relevant information. This is followed by employing reasonable steps to gather and produce documents, after reviewing them for privilege, trade secrets, confidential information or other appropriate bases for non-production.

A similar approach applies to efforts to identify, preserve, and produce relevant information in electronic format. The fact that the information is in a different form does not alter the principle or place a new or greater discovery obligation upon litigants with relevant electronically stored information merely because of the increased volume of potential information involved. Instead, litigants should rely on these traditional foundations for good faith compliance with discovery obligations and employ the unique capabilities of computer tools to assist in identifying, preserving, retrieving, reviewing, and producing relevant electronically stored information and documents.

For further discussion of the requirements for the preservation of electronically stored information, see Principle 5, infra. See also *Principle 8, which suggests practical distinctions in regard to production of electronically stored information based on the methods and characteristics of its storage.*

RESOURCES AND AUTHORITIES

Lee H. Rosenthal, *A Few Thoughts on Electronic Discovery After December 1, 2006,* 116 Yale L.J. Pocket Part 167 (2006).

Shira A. Scheindlin and Jonathan M. Redgrave, *Discovery of Electronic Information, in 2 Bus. & Commercial Litig. in Fed. Courts,* Ch. 22, (Robert L. Haig ed., 2005 & Supp. 2006).

Comment 2.b. Balancing need for and cost of electronic discovery

The proportionality standard of Rule 26(b)(2)(C) requires a balancing of the need for discovery with the burdens imposed and is particularly applicable to electronic discovery. Among the factors pertinent to electronic discovery are: (a) large volumes of data; (b) data stored in multiple repositories; (c) complex internal structures of collections of data and the relationships of one file to another; (d) data in different formats and coding schemes that may need to be converted into text to be reviewed; and (e) frequent changes in information technology. Understanding and generally quantifying these often technical factors are necessary for parties and the court to make reasoned judgments regarding going forward with or limiting discovery.

Electronic discovery burdens should be proportional to the amount in controversy and the nature of the case. Otherwise, transaction costs due to electronic discovery will overwhelm the ability to resolve disputes fairly in litigation.

Costs cannot be calculated solely in terms of the expense of computer technicians to retrieve the data but must factor in other litigation costs, including the interruption and disruption of routine business processes and the costs of reviewing the information. Moreover, burdens on information technology personnel and the resources required to review documents for relevance, privilege, confidentiality, and privacy should be considered in any calculus of whether to allow discovery, and, if so, under what terms. In addition, the non-monetary costs (such as the invasion of privacy rights, risks to business and legal confidences, and risks to privileges) should be considered. Evaluating the need to produce electronically stored information often requires that a balance be struck between the burdens and need for electronically stored information, taking into account the technological feasibility and realistic costs involved.

The Advisory Committee emphasized the importance of the balancing process, quite apart from, and as the underpinning for, the other production limitations. Accordingly, a reference to Rule 26(b)(2)(C) was added to Rule 26(b)(2)(B), and the Committee Note was amended to state that "the limitations [of the rule] continue to apply to all discovery of electronically stored information, including that stored on reasonably accessible electronic sources." Many state courts apply equivalent concepts to reach similar results under existing state rules.

RESOURCES AND AUTHORITIES

Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2008.1 (2d ed. 2006).

McPeek v. Ashcroft, 212 F.R.D. 33, 36 (D.D.C. 2003) (declining to order searches of backup tapes where plaintiff had not demonstrated a likelihood of obtaining relevant information).

Comment 2.c. Limits on discovery of electronically stored information from sources that are not reasonably accessible

Rule 26(b)(2)(B) explicitly limits initial discovery of electronically stored information to information from reasonably accessible sources, the so-called "first tier" of discovery. Reasonably accessible sources generally include, but are not limited to, files available on or from a computer user's desktop, or on a company's network, in the ordinary course of operation.

The converse is information that is "not reasonably accessible" because of undue burden or cost. Examples of such sources may include, according to the Advisory Committee, backup tapes that are intended for disaster recovery purposes and are not indexed, organized, or susceptible to electronic searching; legacy data that remains from obsolete systems and is unintelligible on the successor systems; and data that was "deleted" but remains in fragmented form, requiring a modern version of forensics to restore and retrieve.

A party served with a request for production of electronically stored information from a source that it believes in good faith (a) may contain relevant information but (b) is not reasonably accessible, must identify that source but may object to searching or producing from it. The Rule requires an identification sufficiently detailed to allow the requesting party to evaluate the likelihood that such sources of electronically stored information contain non-duplicative, relevant information as well as the costs and burdens associated with searching or producing electronically stored information from those sources. Importantly, the Rules do not require the identification of all inaccessible sources of electronically stored information, but only those that the producing party believes in good faith may contain relevant, non-duplicative information.

If the parties are unable to reach agreement regarding discovery from such sources, a motion to compel may be brought. In the event of a dispute regarding accessibility, the responding party bears the burden of demonstrating undue burden or cost and may be required to show the specific costs and other elements of the burden. If the responding party meets its burden, the burden shifts to the requesting party to prove that the need for the discovery and the other factors of a "good cause" determination are present for part or all of the discovery requested. The court may permit sampling to assess potential relevance or allow discovery and require that electronically stored information from the data source at issue be produced under appropriate conditions, including the sharing or shifting of costs. The willingness of a requesting party to pay for the additional costs of access, while relevant, is not dispositive.

A producing party may also anticipate a request for production by affirmatively raising issues about its need to preserve or produce information by filing for a protective order that addresses those concerns. Rule 26(b)(2)(B) was revised to explicitly acknowledge that a producing party "may wish to determine its search and potential preservation obligations by moving for a protective order." *See* Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005) *available at* http://www.uscourts.gov/rules/reports/st07-2005.pdf.

For a discussion of the limits of preservation efforts, including those for electronically stored information that is not reasonably accessible, but is reasonably likely to contain potentially relevant information, see *Principle 5. For a discussion of backup tapes,* see *Principle 8. For a discussion of cost shifting in electronic discovery,* see *Principle 13.*

RESOURCES AND AUTHORITIES

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), *available at* http://www.uscourts.gov/rules/reports/st09-2005.pdf.

Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2008.2 (2nd ed. 2006).

Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information, Guideline 1(B)* (August, 2006) (defining "accessible" information as "electronically-stored information that is easily retrievable in the ordinary course of business without undue cost and burden").

Tex. R. Civ. P. 196.4 (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).

Thomas Y. Allman, *The Impact of the Proposed Federal E-Discovery Rules,* 12 Rich. J.L. & Tech. 13 (2006).

Hon. Anthony J. Battaglia, *Dealing with Electronically Stored Information: Preservation, Production, and Privilege,* 53 Fed. Law. 26 (May 2006).

Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure,* 4 Nw. J. Tech. & Intell. Prop. 171 (2006), *available at* http://www.law.northwestern.edu/hournals/njtip/v4/n2/3.

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 319-320 n.61 (S.D.N.Y. 2003) (*"Zubulake I"*) (noting that consideration of cost-shifting is appropriate where stored data is not in a "readily useable" format, such as backup tapes) (noting that Sedona Principles 8 and 9 recognize the distinction between "active data" and backup tapes in a manner very similar to the test employed in the instant case).

Comment 2.d. Need to coordinate internal efforts

Decisions regarding the preservation of electronically stored information should be a team effort, often involving counsel (both inside and outside), information systems professionals, end-user representatives, records and information management personnel, and, potentially, other individuals with knowledge of the relevant electronic information systems and how data is used, such as information security personnel. Parties may also use outside consultants to assist with this process. Such consultants may be included in team activities to the extent consistent with the protection of privileged communications.

The team approach permits an organization to leverage available resources and expertise in ensuring that the organization addresses its preservation and production obligations thoroughly, efficiently and cost-effectively. 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 production of electronically stored information. Of course, the size of the team and the distribution of responsibilities among team members will vary depending upon the size of the organization and the scope of litigation. In short, coordination of information, resources and effort is essential.

For a discussion of the role and risks of counsel in regard to preservation and production of electronically stored information, see *Comment 6f.*

RESOURCES AND AUTHORITIES

Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 431-33 (S.D.N.Y. 2004) (*"Zubulake V"*) (faulting counsel for failing to take adequate steps to preserve data, including failure to interview key players in the litigation about the storage of their documents and failure to take steps beyond issuing the litigation hold to ensure documents were preserved).

Comment 2.e. Communications with opposing counsel and the court regarding electronically stored information

The efficacy of "meet and confers," or other types of communications, depends upon the parties' candor, diligence and reasonableness. A party should accurately represent the complexities and attendant costs and burdens of preservation and production as well as relevance and need for production. Overstated or excessive cost estimates will reduce the organization's credibility, as will vague statements regarding relevance. Further, a producing party should be prepared to present opposing counsel and the court with a reasonable plan for the preservation and production of relevant electronically stored information. When an organization does not present the court with a reasonable plan, the court may err on the side of protecting the integrity of the data collection process and require unnecessary preservation.

Often, neither counsel nor the court will have sufficient technical knowledge to understand the systems at issue. In preparing for court conferences or meet and confer conferences, counsel should consult with their clients' information technology departments and vendors regarding the technical issues involved in data preservation. In turn, organizations should devote sufficient resources to developing presentations that make complex technical issues comprehensible to counsel and the court. When providing affidavits or testimony to counsel or the court on these issues, the organization should be careful to ensure that the affidavits or testimony are not only accurate but also comprehensible to lay individuals with little technical knowledge.

RESOURCES AND AUTHORITIES

Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 113 (2d Cir. 2002) (ineffectiveness of plaintiff's vendor may suggest "purposeful sluggishness" on the part of plaintiff, potentially warranting sanctions on remand).

Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc., No. 502003CA005045XXOCAI, 2005 WL 679071, at *7 (Fla. Cir. Ct. Mar. 1, 2005) *rev'd on other grounds sub nom. Morgan Stanley & Co., Inc. v. Coleman (Parent) Holdings, Inc., ---* So.2d ----, 2007 WL 837221 (Fla. App. 4 Dist. March 21, 2007) (ordering adverse inference instruction against Morgan Stanley and shifting the burden of proof onto the company as sanctions for its destruction of email and non-compliance with the court's prior discovery order, including repeated representations by counsel that Morgan Stanley had thoroughly complied with the court's order); *see also Clare v. Coleman (Parent) Holdings, Inc.,* 928 So. 2d 1246 (Fla. Ct. App. 2006) (reversing lower court's revocation of individual lawyer's pro hac vice status because court's record indicated no misconduct on the part of counsel, who merely acted as messenger from client party in regard to allegations of misconduct regarding spoliation and who was denied due process rights).

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

Comment 3.a. Parties should attempt to resolve electronic discovery issues at the outset of discovery

Early discussion of issues relating to the preservation and production of electronically stored information may help reduce misunderstandings, disputes and unnecessary motions, including post-production sanction motions involving the failure to preserve relevant information. The Federal Rules and a number of local district court rules, as well as increasing numbers of state rules, require that parties engage in such discussions at the outset of any action. Indeed, the Advisory Committee observed that "alert[ing] the court to the possible need to address the handling of discovery of electronically stored information early in the litigation if such discovery is expected to occur" fosters resolution of issues before they cause unnecessary delay and expense on matters unrelated to the merits of the litigation.

An obligation to discuss the issues in good faith applies to both parties, and requesting parties must be prepared to be as precise as possible in regard to potential discovery. So-called "any and all" discovery requests that lack particularity in identifying the responsive time period, subject area, or people involved, should be discouraged, along with blanket objections of "overbreadth." *See* Principle 4, *infra*. Some of the issues that parties should seek to resolve early in an action include: (i) the identification of data sources which will be subject to preservation and discovery; (ii) the relevant time period; (iii) the identities of particular individuals likely to have relevant electronically stored information; (iv) the form or forms of preservation and production; (v) the types of metadata to be preserved and produced; (vi) the identification of any sources of information that are not reasonably accessible because of undue burden or cost, such as backup media and legacy data; (vii) use of search terms and other methods of reducing the volume of electronically stored information to be preserved or produced; and (viii) issues related to assertions of privilege and inadvertent production of privileged documents. The Advisory Committee Note to Rule 26(f) suggests that parties should pay particular attention to achieving a balance between competing needs to preserve relevant evidence and to continue critical routine operations in order to reach agreement on "reasonable preservation steps."

Best practices include the memorializing agreements in writing to guide the parties and, as necessary, informing the court.

> *Illustration i.* In the circumstance of an ongoing preservation obligation, the parties should discuss maintaining select data on a live server or other device and agree upon a process for later review and production.
>
> *Illustration ii.* Plaintiffs in a lawsuit involving allegations of securities fraud against multiple defendants seeking extensive damages request preservation of electronic documents by all defendants. The defendants, most of whom are large investment banks and other financial institutions, respond that preservation obligations need to be tailored so that they are defined, manageable, and cost-effective while also preserving evidence that is truly needed for the resolution of the dispute. The parties meet and confer upon a protocol for preserving existing data, including preserving select (not all) backup tapes, certain archived data, and select legacy systems; distributing retention notices (and updates); creating a limited number of mirror images of select computer hard drives; undertaking measures to collect potentially relevant data; and distributing a questionnaire regarding electronic data systems. The defendants assess the costs and burdens involved in the various proposed steps and reach agreement on the scope and limitations of the obligations. The protocol averts motion practice and provides certainty as to the expected preservation efforts.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 16(b)(5), 26(f)(3) (requiring that electronically stored information be a topic of the initial meet and confer and discovery plan).

Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information,* Guideline 3 (Aug. 2006).

Manual for Complex Litigation (*Fourth*), § 40.25(2) (Fed. Jud. Ctr. 2004) (providing a list of considerations for electronically stored information discovery conferences).

D. Kan. *Guidelines for Discovery of Electronically Stored Information* (parties have a duty to disclose, as part of the Fed. R. Civ. P. 26(f) conference, any electronically stored information that may be used to support a claim or defense; steps that will be taken to preserve electronically stored information; whether embedded data or metadata exist and, if so, the extent to which it will be produced and how the parties will address issues of privilege; whether restoration of backups is needed and who will bear the costs; the format and media of production; and how inadvertently disclosed privileged materials will be treated.).

D.N.J. L. R. 26.1(d) (counsel have a duty to investigate a client's information management systems and identify persons with knowledge of those systems and shall confer and attempt to agree on preservation and production of digital information and who will bear the costs of preservation, production, and restoration of any digital discovery).

Treppel v. Biovail Corp., 233 F.R.D. 363, 374 (S.D.N.Y. 2006) (stressing the importance of reaching early agreements, including use of preservation orders, on topics which could become contentious in post-production disputes and criticizing failure to discuss potential search terms).

In re Bristol-Myers Squibb Sec. Litig., 205 F.R.D. 437, 441, 444 (D.N.J. 2002) (holding that Fed. R. Civ. P. 26(a)(1) requires a party to disclose the existence of electronic information at the time it makes initial disclosures and that the Fed. R. Civ. P. 26(f) "meet and confer should include a discussion on whether each side possesses information in electronic form, whether they intend to produce such material, whether each other's software is compatible, whether there exists any privilege issue requiring redaction, and how to allocate costs involved with each of the foregoing.").

Comment 3.b. Procedural issues relating to form of production

Federal Rule of Civil Procedure 26(f) calls for an early discussion of form of production issues. Rule 34 sets forth a more detailed explanation of the ways in which parties should request and respond to requests seeking production or inspection of electronically stored information.

At the outset, parties seeking discovery should have sufficient technical knowledge of production options so that they can make an educated and reasonable request. These should be discussed at the Rule 26(f) conference and included in any Rule 34(a) requests. Likewise, responding parties should be prepared to address form of production issues at the Rule 26(f) conference.

With respect to requests and responses, the revised Rule 34(b) provides that a request may specify the form or forms in which electronically stored information is to be produced. If objection is made to the requested form or forms for producing electronically stored information, or if no form was specified in the request, the responding party must state the form or forms it intends to use.

If a request does not specify the form or forms for producing electronically stored information, and absent agreement of the parties, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable unless otherwise ordered by the court. A party need not produce the same electronically stored information in more than one form.

Significantly, the Committee Note to amended Rule 34 makes clear that the option to produce in a "reasonably usable form" does not mean that a responding party is free to convert electronically stored information from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to search and review the documents. Parties and counsel will need to carefully consider the ways in which they preserve and produce documents to ensure that they will be able to realize Rule 34's goal of a fair and reasonable approach to the form of production.

For a discussion of the metadata issue in the context of discovery, see *Principle 12,* infra.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 34 (governing the form of production).

Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information,* Guideline 6 (Aug. 2006).

ABA Civil Discovery Standards (1999) (rev. Aug. 2004), Standard 29(b)(ii)(A), *available at* http://www.abanet.litigation/discoverystandards/2004civildiscoverystandards.pdf.

Craig Ball, *Understanding Metadata: Knowing Metadata's Different Forms and Evidentiary Significance is Now an Essential Skill for Litigators,* 13 L. Tech. Prod. News 36 (Jan. 2006).

Sattar v. Motorola, Inc., 138 F.3d 1164, 1171 (7th Cir. 1998) (affirming district court's denial of plaintiff's motion to compel hard copies of over 200,000 emails even though plaintiff's system was unable to read defendant's electronic files, because a more reasonable accommodation was (i) some combination of downloading the data from the tapes to conventional computer disks, (ii) loaning plaintiff a copy of the necessary software, or (iii) offering plaintiff on-site access to its own system).

Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 652 (D. Kan. 2005) (*"Williams I"*)("When a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to the production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order.").

Comment 3.c. Privilege logs for voluminous electronically stored information

In litigations with a large volume of relevant, non-duplicative paper documents and electronically stored information, the volume of privileged information may be correspondingly large. The applicable rule states the following:

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

Fed. R. Civ. P. 26 (b)(5)(A).

Traditionally, parties have complied with this rule by producing a privilege log with separate entries for each document that contain objective information about the document (such as author, addressee and Bates number) as well as a field that describes the basis for the privilege claim. Even if there are few documents, preparing a privilege log is often extremely time-consuming. Even with the best efforts of counsel, it often results in a privilege log that is of marginal utility at best. The immense volume of electronic documents now subject to discovery exacerbates the problem.

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

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

Fed. R. Civ. P. 26 Committee Note (1993).

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

Comment 3.d. Preservation of expert witness drafts and materials

The obligation to preserve and produce electronically stored information may apply to expert witness materials. The 1993 amendments to Rule 26(a)(2)(B) require the disclosure of all "information considered by the [expert] in forming the [expert's] opinion." Under this standard, courts have held that the failure to preserve information could lead to sanctions and the exclusion of testimony. It is not hard to imagine that litigants will quickly adapt the electronic spoliation disputes of document discovery to the realm of expert witness disclosures (for example, requests for all of the electronic copies of expert witness reports, for access to the expert's hard drive to search for deleted data, or requests for access to all email accounts of the expert).

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

RESOURCES AND AUTHORITIES

The Sedona Conference Commentary on the Role of Economics in Antitrust Law (June 2006), Principle II-2 ("The process by which an economic opinion is reached can and should be shielded from discovery.").

Gabrielle R. Wolohojian & David A. Giangrasso, *Expert Discovery and the Work Product Doctrine – Is Anything Protected?* 48-APR B. B.J. 10 (Mar./Apr. 2004).

Trigon Ins. Co. v. United States, 204 F.R.D. 277, 282-84, 289-91 (E.D. Va. 2001) (finding that government had duty to preserve correspondence between experts and consultants, including drafts of expert reports; that the destruction of such evidence was intentional, warranting sanctions for spoliation of evidence; and that an adverse inference instruction regarding the experts' testimony and their credibility in general was warranted).

4. Discovery requests for electronically stored information should be as clear as possible, while responses and objections to discovery should disclose the scope and limits of the production.

Comment 4.a. Requests for production should clearly specify what electronically stored information is being sought

A requesting party that seeks production of electronically stored information should, to the greatest extent practicable, clearly and specifically indicate the types of electronic information it seeks. Such discovery requests should go beyond boilerplate definitions seeking all email, databases, word processing files, or whatever other electronically stored information the requesting party can generally describe. Instead, the request should target particular electronically stored information that the requesting party contends is important to resolve the case. By identifying relevant individuals and topics, parties can avoid the sort of blanket, burdensome requests for electronically stored information that invite blanket objections and judicial intervention.

The requesting party should also identify the form or forms in which it wishes the electronically stored information to be produced, and, if it deems it important or useful, any particular fields or types of metadata sought. A request for production of electronically stored information in the form in which it is maintained should be interpreted as seeking production in native format, with all relevant metadata, and a producing party should object or otherwise raise its concerns if it is not prepared to make production in that form. An early discussion of the potential form or forms of production is advisable in order to permit planning for preservation steps and to identify any disputes that may have to be resolved. *See* Principles 3 *infra* and Principle 12, *supra*.

In federal cases, the subject of form of production must be discussed at the Rule 26(f) conference. If agreement is reached, it may be embodied in a Rule 16(b) Scheduling Order. If the parties do not reach agreement or the court is not asked to resolve the matter, the producing party may use one of two "default forms," either the form "in which it is ordinarily maintained," or a form that is "reasonably usable." Fed. R. Civ. P. 34(b)(2).

For a more detailed discussion of the process and advantages related to a particular form of production, including a discussion of the role of metadata, see *Comment 3.c and Comment 12.a.*

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 34 Committee Note (2006) (Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and 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.).

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.").

Wright v. AmSouth Bancorp., 320 F.3d 1198, 1205 (11th Cir. 2003) (holding that trial court did not abuse its discretion by finding plaintiff's request for "computer diskette or tape copy of all word processing files created, modified and/or accessed by, or on behalf" of five employees of the defendant over a two-and-one-half-year period as overly broad in scope, unduly burdensome, and not reasonably related to the plaintiff's age discrimination claims).

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 321-22 (S.D.N.Y. 2003) ("*Zubulake I*") (noting that specificity is the touchstone of any good discovery request and holding that one factor to consider when deciding whether to shift costs of production of electronic evidence is "the extent to which the request is specifically tailored to discover relevant information").

Comment 4.b. Responses and objections

Responses and objections should clearly and specifically state all objections and should also indicate the extent to which production of relevant electronically stored information will be limited, based on undue burden or cost of production efforts, not restricted to those sources of information identified as "not reasonably accessible."

It is neither reasonable nor feasible for a party to search or produce information from every electronic file that might potentially contain information relevant to every issue in the litigation, nor is a party required to do so. It should be reasonable, for example, to limit searches for email messages to the 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 files of key individuals. Likewise, it should be appropriate, absent unusual circumstances, to limit review for production to those sources most likely to contain nonduplicative relevant information (such as active files or removable media used by key employees). The use of search terms may assist in reducing the volume of information that must be further reviewed for relevance and privilege.

In cases governed by the Federal Rules, a producing party that does not intend to produce relevant electronically stored information from sources identified as not reasonably accessible because of undue burden or cost must identify those sources to the requesting party. *See* Fed. R. Civ. P. 26(b)(2)(B). Absent local rule or a court order, this Rule does not require the specificity of a traditional privilege log, nor does it require the listing of electronic information systems or storage devices that have not been identified as a source of nonduplicative, relevant information.

If the requesting party did not specify a form or forms for the requested production, or the responding party objects the form or forms requested, the responding party must identify the form or forms it intends to use. If the requesting party specified a form or forms for the requested production, the responding party should either note agreement or include an objection and then identify the form or forms it intends to use. *See* Fed. R. Civ. P. 34(b).

The better practice is to discuss and attempt to agree upon such practical limitations in responses so that any disputes can be addressed and resolved early.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 34 (specifying that requester may designate form in which production is to occur).

Tex. R. Civ. P. 193.2(a) (to object to a discovery request, the responding party must make a timely objection in writing and state specifically the legal or factual basis for the objection and the extent to which the party is refusing to comply with the request).

In re Ford Motor Co., 345 F.3d 1315, 1317 (11th Cir. 2003) (stating that the producing party's choice to review database and only produce those relevant portions was adequate discovery response absent specific evidence to the contrary).

Thompson v. U.S. Dep't of Hous. & Urban Dev., 219 F.R.D. 93, 98-99 (D. Md. 2003) (stating that "[c]onclusory or factually unsupported assertions by counsel that the discovery of electronic materials should be denied because of burden or expense can be expected to fail" and noting that the producing party was previously cautioned that its objections to producing electronic records would have to be "particularized" with an affidavit that "identifies evidentiary facts to support the claims of unfair burden or expenses").

Comment 4.c. Meet and confer obligations relating to search and production parameters

It is usually not feasible, and may not even be possible, for most business litigants to collect and review all data from their computer systems in connection with discovery. The extraordinary effort that would be required to do so could cripple many businesses. Yet, without appropriate guidelines, if any data is omitted from a production, an organization may be accused of withholding data that should have been produced, and if that data is not preserved, of spoliation. Unnecessary controversy over peripheral discovery issues can often be avoided at the outset by discussion by the parties of the potential scope and related costs of collecting relevant data. Accordingly, and consistent with the amended Federal Rules and best practices, parties should be prepared to discuss the sources of electronically stored information that have been identified as containing relevant information, as well as the steps that have been taken to search for, retrieve, and produce such information.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 26(f) (requiring parties to address issues associated with electronic production at an early stage in litigation).

Fed. R. Civ. P. 16(b)(5), 16(b)(6) (adapting scheduling order to include provisions relating to electronically stored information).

5. The obligation to preserve electronically stored information 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 electronically stored information.

Comment 5.a. Scope of preservation obligation

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

The preservation obligation necessarily involves two related questions: (1) when does the duty to preserve attach, and (2) what evidence, including potentially discoverable electronically stored information, must be preserved. The first inquiry remains unchanged from prior practice. In the world of electronically stored information, the need to recognize when the duty has been triggered may be more important with respect to those electronic information systems that quickly delete or overwrite data in the ordinary course of operations.

The second inquiry presents a much greater challenge with respect to electronically stored information than with paper. The obligation to preserve relevant evidence is generally understood to require that the producing party make reasonable and good faith efforts to identify and manage the information that it has identified as reasonably likely to be relevant. Satisfaction of this obligation must be balanced against the right of a party to continue to manage its electronic information in the best interest of the enterprise, even though some electronic information is necessarily overwritten on a routine basis by various computer systems. If such overwriting is incidental to the operation of the systems – as opposed to a deliberate attempt to destroy evidence in anticipation of or in connection with an investigation or litigation – it should generally be permitted to continue after the commencement of litigation, unless the overwriting destroys potentially discoverable electronic information that is not available from other sources.

Just as organizations need not preserve every shred of paper, they also need not preserve every email or electronic document, and every backup tape. To require such broad preservation would cripple entities which are almost always involved in litigation and make discovery even more costly and time-consuming. A reasonable balance must be struck between (1) an organization's duty to preserve relevant evidence, and (2) an organization's need, in good faith, to continue operations. *See* Fed. R. Civ. P. 37(f).

> *Illustration i.* L Corporation ("L Corp.") routinely backs up its *email* 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 *emails* relating to the issues in the litigation, and the legal department takes reasonable steps to ensure that all relevant evidence has, in fact, been preserved. L Corp. continues its policy of recycling backup tapes while the litigation is pending. Absent awareness of a reasonable likelihood that specific unique and relevant information is contained only on a backup tape, there is no violation of preservation obligations, because the corporation has an appropriate policy in place and the backup tapes are reasonably considered to be redundant of the data saved by other means.

For a discussion of the duty to preserve information which is found on sources identified as not reasonably accessible because of undue burden or cost, see *Comment 5.b. ("Organizations must prepare for electronic discovery to reduce cost and risk") and Comment 5.h. ("Disaster recovery backup tapes").*

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 37(f).

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), *available at* http://www.uscourt.gov/rules/reports/st09-2005.pdf.

Ronald J. Hedges, *Discovery of Electronically Stored Information: Surveying the Legal Landscape,* 86-91 (BNA Books 2007) (discussing circumstances in which preservation obligations may arise).

Thomas Y. Allman, *Defining Culpability: The Search for A Limited Safe Harbor in Electronic Discovery,* 2006 Fed. Cts. L. Rev. 7 (2006).

Maria Perez Crist, *Preserving the Duty to Preserve: The Increasing Vulnerability of Electronic Information,* 58 S.C. L. Rev. 7 (2006).

Richard L. Marcus, *Confronting the Future: Coping with Discovery of Electronic Material,* 64-SUM L. & Contemp. Probs. 253, 267-68 (2001).

Martin H. Redish, *Electronic Discovery and the Litigation Matrix,* 51 Duke L.J. 561, 621 (2001).

7 Moore's Federal Practice Section 37A.12[5][e] (3d ed. 2006) ("The routine recycling of magnetic tapes that may contain relevant evidence should be immediately halted on commencement of litigation.").

When Duty to Preserve Arises:

Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 748 (8th Cir. 2004) (spoliation found when train company failed to produce cab voice tapes following a fatal crash because the railroad knew that fatal crashes frequently lead to litigation and the voice tapes were particularly crucial pieces of evidence).

Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998) (The "obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation – most commonly when suit has already been filed, providing the party responsible for the destruction with express notice, but also on occasion in other circumstances, as for example when a party should have known that the evidence may be relevant to future litigation.").

Testa v. Wal-Mart Stores, Inc., 144 F.3d 173, 177-178 (1st Cir. 1998) (duty to preserve arises at a time measured by the "institutional notice – the aggregate knowledge possessed by a party and its agents, servants and employees").

Silvestri v. General Motors Corp., 271 F.3d 583, 591 (4th Cir. 2001) (holding that the duty to preserve evidence arises when the party knows or reasonably should know that the evidence may be relevant to pending or anticipated future litigation).

Fujitsu Ltd. v. Federal Express Corp., 247 F.3d 423, 436 (2d Cir. 2001) (holding that "[t]he obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation").

Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 216-17 (S.D.N.Y. 2003) (*"Zubulake IV"*) (in employment discrimination case, duty to preserve attached as soon as plaintiff's supervisors became reasonably aware of the possibility of litigation, rather than when EEOC complaint was filed several months later).

Rambus, Inc. v. Infineon Techs. AG, 220 F.R.D. 264 (E.D. Va. Mar. 17, 2004), subsequent determination, 222 F.R.D. 280 (May 18, 2004) (the duty to preserve evidence arises before litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation; thus, once a party reasonably anticipates litigation, it must suspend any routine document purging system, and put in place a litigation hold to ensure the preservation of relevant documents; concomitantly, there is a duty not to initiate a document destruction regime that may result in the destruction of potentially relevant information if a party reasonably anticipates litigation); *see also Samsung Elecs. Co. v. Rambus, Inc.,* 439 F. Supp. 2d 524 (E.D. Va. 2006) (finding that Rambus' destruction of evidence at a time when it anticipated litigation could form the basis of a finding of exceptionality within the meaning of the patent statute authorizing attorney's fees in exceptional cases); *Hynix Semiconductor Inc. v. Rambus, Inc.,* No. C-00-20905 RMW, 2006 WL 565893 (N.D. Cal. Jan. 5, 2006) (finding no spoliation or bad faith in implementation of document management and destruction policy because litigation was not "probable" at the time the party introduced the policy, as the "path to litigation was neither clear nor immediate" at that time).

Scope of Duty to Preserve:
Mosaid Techs. Inc. v. Samsung Elecs. Co., 348 F. Supp. 2d 332, 336 (D.N.J. 2004) (while a litigant is under no duty to keep or retain every document in its possession, even in advance of litigation, it is under a duty to preserve what it knows, or reasonably should know, will likely be requested in reasonably foreseeable litigation).

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 324 (S.D.N.Y. 2003) (*"Zubulake I"*) (plaintiff entitled to all emails and electronic documents relevant to employment discrimination claim, including those only preserved on backup tapes; however, given burden and expense of restoring inaccessible backup tapes, a cost-shifting analysis is appropriate).

Concord Boat Corp. v. Brunswick Corp., No. LR-C-95-781, 1997 WL 33352759, at *4 (E.D. Ark. Aug. 29, 1997) (corporation fulfilled duty to preserve by retaining all relevant emails subsequent to the filing of the complaint and the preservation order, but not all emails prior to litigation: "to hold that a corporation is under a duty to preserve all email potentially relevant to any future litigation would be tantamount to holding that the corporation must preserve all email;" such a holding, the court found, would be crippling to large corporations, which are often involved in litigation).

Comment 5.b. Organizations must prepare for electronic discovery to reduce cost and risk

The main purpose of computer systems is to assist the organization in its business activities. Nonetheless, the need to respond to discovery in litigation is a fact of life for many organizations. Preparing in advance for electronic discovery demands can greatly ease the burdens and risk of inaccuracy inherent in efforts to prepare for initial disclosures and meet and confer sessions once litigation begins. In addition, the accessibility of information and the costs of responding to requests for discovery of information contained in computer systems can be best controlled if the organization takes steps ahead of time to coordinate with and prepare IT staff, records management personnel, managers, and users of these systems for the potential demands of litigation. Preparing for electronic discovery can also help the organization reasonably calculate the cost and burden of discovery requests, control production costs, and minimize the risk of failing to preserve or produce relevant information from computer systems.

Such steps include instituting defined policies and procedures for preserving and producing potentially relevant information, and establishing processes to identify, locate, preserve, retrieve, and produce information that may be relevant or required for initial mandatory disclosures. Organizations should provide training regarding these policies and procedures.

> *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 *email*, 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. Plaintiffs' counsel obtains an *ex parte* order requiring Med to save all of its backup tapes, to refrain from using any auto-deletion functions on *email* 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 complying with the order will cost at least $150,000 per month, including the cost of new tapes, reconfiguration of backup procedures and tape storage, purchase and installation of additional hard drive space for accumulating *email* 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.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 26(b)(2)(B).

Fed. R. Civ. P. 37(f) Committee Note (2006) ("Whether good faith would call for steps to prevent the loss of information on sources that the party believes are not reasonably accessible under Rule 26(b)(2)(B) depends upon the circumstances of each case. One factor is whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources.").

Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) *("Zubulake IV")*, (parties must retain all relevant documents in existence or created after the duty to preserve attaches, but organizations need not preserve "every shred of paper, every email or electronic document, and every back-up tape").

Comment 5.c. Corporate response regarding litigation preservation

Organizations should define the scope of their preservation obligations as soon as practicable after the duty to preserve arises. Failure to initiate reasonable preservation protocols as soon as practicable may increase the risk of disputes that relevant information was not preserved. In so doing, the execution of what has come to be known as a "litigation hold" is advisable, to provide a repeatable, documented process to assist in meeting preservation obligations.

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 defenses, and the information at issue. That said, organizations addressing preservation issues should carefully consider likely future discovery demands for relevant electronically stored information to avoid needless repetitive steps to capture data again in the future. Ideally, an effective process to identify and retain documents and electronically stored information reasonably subject to the preservation obligation should be established as soon as practicable. An appropriate notice should be effectively communicated to those employees and others likely to have or know of such information. Senior management and legal advisors should be involved in the retention decisions and processes.

RESOURCES AND AUTHORITIES

Gregory G. Wrobel, *et al., Counsel Beware: Preventing Spoliation of Electronic Evidence in Antitrust Litigation,* 20-SUM Antitrust 79 (2006).

Mafe Rajul, *"I Didn't Know My Client Wasn't Complying!" The Heightened Obligation Lawyers Have to Ensure Clients Follow Court Orders in Litigation Matters,* 2 Shidler J.L. Com. & Tech. 9 (2005).

Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) (*"Zubulake V"*) (faulting counsel for failing to interview key players in litigation or do keyword search of databases in course of creating and enforcing litigation hold).

Rambus, Inc. v. Infineon Tech. AG, 220 F.R.D. 264 (E.D. Va. Mar. 17, 2004), *subsequent determination*, 222 F.R.D. 280 (May 18, 2004) (duty not to initiate a document destruction regime if a party reasonably anticipates litigation).

Comment 5.d. Preservation notice to affected persons ("legal holds")

Upon determining that litigation or an investigation is threatened or pending and has triggered a preservation obligation, the organization should take reasonable steps to communicate the need to preserve information to appropriate persons, except when particular circumstances make hold notices unnecessary or inadvisable.

The recipient list will include persons responsible for maintaining information potentially relevant to that litigation or investigation. The list may also include the person or persons responsible for maintaining and operating computer systems or files, including back-up and archiving systems, which may fall within the scope of the preservation obligation. The notice does not need to reach all employees, only those reasonably likely to maintain documents relevant to the litigation or investigation. In many cases, the notice should be sent to a person or persons responsible for maintaining and operating computer systems or files that have no particular custodian or owner but may fall within the scope of the preservation obligation.

While the form and content of the notice may vary widely depending upon the circumstances, the notice need not provide a detailed list of all information to retain. Instead, it should describe the types of information that must be preserved, with enough detail to allow the recipient to implement the hold. The notice should state that electronically stored information, as well as paper, are subject to the need for preservation. Additionally, the notice should: (i) describe the subject matter of the litigation and the subject matter, dates, and other criteria defining the information to be preserved; (ii) include a statement that relevant electronically stored information and paper documents must be preserved; (iii) identify likely locations of relevant information (e.g., network, workstation, laptop or other devices); (iv) provide steps that can be followed for preserving the information as may be appropriate; and (v) convey the significance of the obligation to the recipients.

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.

Communications should be accomplished in a manner reasonably designed to provide prominent notice to the recipients. Depending on the scope and duration of the litigation, it may be advisable to repeat such notice. When preservation obligations apply to documents and data spanning a significant or continuing time period, organizations should analyze whether special steps are needed to preserve unique, relevant electronic information stored on outdated or retired systems.

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

Parties also should consider whether notice must be sent to third parties, such as contractors and vendors, including those that provide information technology services. This concern arises out of Rule 34, which frames a party's obligation in terms of its possession, custody, or control of documents.

It must be recognized that in some circumstances, a legal hold notice may be unnecessary (e.g., the relevant information is already secured) or inadvisable (e.g., the notice itself may trigger evidence destruction efforts by the employee under investigation).

Comment 5.e. Preservation obligation not ordinarily heroic or unduly burdensome

The preservation obligation does not ordinarily impose heroic or unduly burdensome requirements on organizations with respect to electronically stored information, although a party may request, and a court can compel, the exercise of extraordinary efforts to preserve electronically stored information even if it is not reasonably accessible in the ordinary course of business, or is particularly transitory and costly and burdensome to preserve. The obligation to preserve normally requires reasonable and good faith efforts. The obligation to undertake extraordinary efforts should be exercised only when there is a substantial likelihood that the information exists; that it would not remain in existence absent intervention; that the information (or its substantial equivalent) cannot be found in another, more accessible data source; and that its preservation is likely to materially advance the resolution of the litigation in a just, efficient, and relatively inexpensive manner.

> *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.

RESOURCES AND AUTHORITIES

Fed. R. Civ. P. 26(b)(2) ("The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that … the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.").

Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2008.1 (2d ed. 2006).

Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162, 177 (S.D.N.Y. 2004) (relying on proposed amendment to Fed. R. Civ. P. 37(f) in holding preservation efforts would have required "heroic efforts far beyond those consistent with [defendants] regular course of business," since the data in question were "ephemeral," existing only until the tuning engineer made the next adjustment).

Comment 5.f. Preservation orders

In general, courts should not issue a preservation order over objection unless the party requesting such an order demonstrates its necessity, which may require an evidentiary hearing in some circumstances. Because all litigants are obligated to preserve relevant evidence in their possession, custody, or control, a party seeking a preservation order must first demonstrate a real danger of evidence destruction, the lack of any other available remedy, and that a preservation order is an appropriate exercise of the court's discretion.

That said, jointly stipulated preservation orders may aid the discovery process by defining the specific contours of the parties' preservation obligations. Before any preservation order is issued, the parties should meet and confer to discuss the scope and parameters of the preservation obligation. Whether agreed to or ordered over objection, preservation orders should be narrowly tailored to require preservation of documents and electronically stored information that are nonduplicative and relevant to the case, without unduly interfering with the normal functioning of the affected party's operations and activities, including the operation of electronic information systems.

Ex parte preservation orders should rarely be entered. Such orders violate the principle that responding parties are responsible for preserving and producing their own electronically stored information. More generally, preservation orders rarely should be issued over objection, and only after a full and fair opportunity to present evidence and argument. This is particularly important when dealing with electronically stored information that may be transitory, not reasonably accessible, or not susceptible to reasonable preservation measures.

Usually, neither the party seeking a preservation order nor the court will have a thorough understanding of the other parties' computer systems, 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 and technologies vary greatly. Without information about the specifics of the backup system in use, it is difficult to tell what steps are reasonable to meet the needs of the case.

The 2006 amendments to the Federal Rules carefully balance the need to discourage unnecessary, premature and/or overbroad preservation orders with the need to prevent the loss of information important to the litigation and to help parties who sought to memorialize agreements on the scope of their preservation obligations. As set forth in the Committee Note to Rule 26(f), "the requirement that the parties discuss preservation does not imply that courts should routinely enter preservation orders. A preservation order entered over objections should be narrowly tailored. *Ex parte* preservation orders should issue only in exceptional circumstances." Rule 26(b)(2)(B) was also amended to make it clear that either party may seek immediate relief in connection with preservation obligations.

RESOURCES AND AUTHORITIES

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), *available at* http://www.uscourts.gov/rules/reports/st09-2005.pdf (Fed. R. Civ. P. 26(b)(2)(B) text has been changed to recognize that the responding party may wish to determine its search and potential preservation obligations by moving for a protective order (C-50) and Fed. R. Civ. P. 37(f) "exemption [for violation of protective orders] was deleted for fear that it would invite routine applications for protective orders, and often over broad orders" (C-88-89.).

Manual for Complex Litigation (*Fourth*), § 11.442 (Fed. Jud. Ctr. 2004).

Capricorn Power Co. v. Siemens Westinghouse Power Corp., 220 F.R.D. 429, 433-34 (W.D. PA. 2004) (discussing new balancing test to be used to evaluate necessity of preservation order, which looks at: "1) the level of concern the court has for the continuing existence and maintenance of the integrity of the evidence in question in the absence of an order directing preservation of the evidence; 2) any irreparable harm likely to result to the party seeking the preservation of evidence absent an order directing preservation; and 3) the capability of an individual, entity, or party to maintain the evidence sought to be preserved, not only as to the evidence's original form, condition or contents, but also the physical, spatial and financial burdens created by ordering evidence preservation").

Comment 5.g. All data does not need to be "frozen"

A party's preservation obligation does not require "freezing" of all electronically stored information, including all email. Organizations need not preserve "every shred of paper, every email or electronic document, and every back-up tape," nor do they have to go to extraordinary measures to preserve "all" potentially relevant evidence.

Civil litigation should not be approached as if information systems were crime scenes that justify forensic investigation at every opportunity to identify and preserve every detail. Theoretically, a party could preserve the contents of waste baskets and trash bins for evidence of statements or conduct. Yet, the burdens and costs of those acts are apparent and no one would typically argue that this is required. There should be a similar application of reasonableness to preservation of electronic documents and data.

Even though it may be technically possible to capture vast amounts of data during preservation efforts, this usually can be done only at great cost. Data is maintained in a wide variety of formats, locations and structures. Many copies of the same data may exist in active storage, backup, or archives. Computer systems manage data dynamically, meaning that the

data is constantly being cached, rewritten, moved and copied. For example, a word processing program will usually save a backup copy of an open document into a temporary file every few minutes, overwriting the previous backup copy. In this context, imposing an absolute requirement to preserve all information would require shutting down computer systems and making copies of data on each fixed disk drive, as well as other media that are normally used by the system. Costs of litigation would routinely approach or exceed the amount in controversy. In the ordinary course, therefore, the preservation obligation should be limited to those steps reasonably necessary to secure evidence for the fair and just resolution of the matter in dispute.

> *Illustration i.* In a Freedom of Information Act ("FOIA") action, the district court enters a preliminary injunction that the agency believes requires it to freeze all computers that could potentially contain documents subject to the FOIA dispute. In implementing the order, the agency determines that the categorical freeze on all agency hard drives requires the purchase of new equipment with each personnel change and wherever there are certain types of equipment malfunctions. The agency should approach the court for implementation of a more limited order so that only those computers that contain responsive records will be preserved and all others can be released for reuse.

RESOURCES AND AUTHORITIES

Thomas Y. Allman, *Defining Culpability: The Search for A Limited Safe Harbor in Electronic Discovery,* 2006 Fed. Cts. L. Rev. 7 (2006).

Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) (*"Zubulake IV"*) (parties must retain all relevant documents in existence or created after the duty to preserve attaches, but organizations need not preserve "every shred of paper, every email or electronic document and every back-up tape").

Manual for Complex Litigation (Fourth), Sample Order 40-25 (Fed. Jud. Ctr. 2004) (broad interim protective order intended to encourage the parties to negotiate a more permanent stipulated order).

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

In some organizations, however, the concepts of backup and archive are not clearly separated, and backup tapes are retained for a relatively long time period to retain files that may need to be accessed in the future. Backup tapes may also be retained for long periods out of concern for compliance with record retention laws. Under these circumstances, the stored backup tapes may contain the only remaining copy of relevant data or documents. 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, consider employing means other than traditional disaster recovery backup tapes. They should not be used for recordkeeping.

> *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 significant expenses and burdens on the producing party, which are documented in factual submissions. No credible evidence is shown establishing the likelihood that, absent the requested order, the producing party will not produce all relevant information during discovery. The producing party should be permitted to continue the routine recycling of backup tapes in light of the expense, burden and potential complexity of restoration and search of the backup tapes.

Finally, if it is unclear whether there is a reasonable likelihood that nonduplicative, relevant information is contained on backup tapes, the parties and/or the court may consider the use of sampling to better understand the nature and relevance of the information at issue. Depending on the circumstances of the case, sampling may establish that there is very little, if any, unique, relevant information on the tapes, and that there is no need for the tapes to be retained or restored. Similarly, sampling may establish that it is reasonable to retain and restore only certain intervals of available tapes to satisfy the party's good faith compliance with its preservation and production obligations.

> *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.

According to the Report of the Civil Rules Advisory Committee presenting the proposed amendments to the Federal Rules, disaster recovery tapes which are "intended for disaster recovery purposes that are often not indexed, organized, or susceptible to electronic searching" are identified as sources that may not reasonably be accessible and therefore are not subject to initial production absent a court order. However, a party will need to disclose backup tapes that it determines are not reasonably accessible if it has a reasonable, good faith belief that relevant, non-duplicative data reside on those tapes; and, therefore, the Rule assumes the preservation of such backup tapes.

RESOURCES AND AUTHORITIES

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), C-42 *available at:* http://www.uscourts.gov/rules/reports/st09-2005.pdf (giving examples from "current technology").

Fed. R. Civ. P. 26 (b)(2)(B) Committee Note, ("A party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence. Whether a responding party is required to preserve unsearched sources of potentially responsive information that it believes are not reasonably accessible depends on the circumstances of each case.").

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), C-83 *available at* http://www.uscourts.gov/rules/reports/st90-2005.pdf. ("Examples of [routine operations] include programs that recycle storage media kept for brief periods against the possibility of a disaster that broadly affects computer operations").

Fed. R. Civ. P. 37(f) Committee Note (2006) ("One factor [in deciding whether to interrupt programs] is whether the party reasonably believes that the information on such sources is likely to be discoverable and not available from reasonably accessible sources.").

7 Moore's Federal Practice § 37A.12[5][e] (3d ed. 2006) ("The routine recycling of magnetic tapes that may contain relevant evidence should be immediately halted on commencement of litigation.").

36 C.F.R. 1234.24(c)(2006) ("[B]ackup tapes should not be used for recordkeeping purposes.").

McPeek v. Ashcroft, 202 F.R.D. 31, 33 (D.D.C. 2001) ("There is certainly no controlling authority for the proposition that restoring all backup tapes is necessary in every case. The Federal Rules do not require such a search, and the handful of cases is idiosyncratic and provides little guidance.").

Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217-18 (S.D.N.Y. 2004) (*"Zubulake IV"*) (concluding that "'as a general rule, then, a party need not preserve all backup tapes even when it reasonably anticipates litigation. … However, it does make sense to create one exception to this general rule. If a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of 'key players' to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available.").

Comment 5.i. Preservation of shared and orphaned data

An organization's networks or intranet may contain shared areas (such as public folders, discussion databases and shared network folders) that are not regarded as belonging to any specific employee. There are also collaborative work space areas (such as blogs, wikis, and intranet sites) where there is no one "owner" of the data within the organization. Such areas should be considered in the preservation and analysis to determine if they contain potentially relevant information and, if so, appropriate steps should be taken to preserve the relevant information.

If an organization maintains archival data on tapes 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 also present as active data on the organization's systems. These steps may include notifying persons responsible for managing archival systems to retain tapes or other media as appropriate.

6. Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information.

Comment 6.a. The producing party should determine the best and most reasonable way to locate and produce relevant information in discovery

It is the responsibility of the producing party to determine what is responsive to discovery demands and to make adequate arrangements to preserve and produce relevant information. There are various ways to manage electronic documents, and thus many ways in which a party may comply with its obligations. The failure to do so in an organized and methodical fashion, however, has led some courts to impose penalties upon both the party and the responsible employee.

Typically, the producing party identifies and informs the key individuals likely to have relevant information of the specific need to preserve all available relevant information – this instruction is sometimes referred to as a "litigation hold notice." Thereafter, the lawyers supervise the collection of the relevant information from custodians and other sources. The party then conducts a review for privilege, trade secrets, or other appropriate bases for nonproduction and takes reasonable steps to facilitate production A producing party should not be required to undertake more heroic efforts merely because the party seeking discovery is suspicious of the efforts undertaken by the producing party.

RESOURCES AND AUTHORITIES

In re Ford Motor Co., 345 F.3d 1315, 1317 (11th Cir. 2003) (stating that the producing party's choice to review database and only produce those relevant portions was adequate discovery response absent specific evidence to the contrary).

Comment 6.b. Scope of collection of electronically stored information

When responding to discovery requests, organizations should define the scope of the electronically stored information needed to appropriately and fairly address the issues in the case and to avoid unreasonable overbreadth, burden, and cost. Important steps in achieving the goal of reasonably limiting discovery may include: (1) collecting electronically stored information from repositories used by key individuals rather than generally searching through the entire organization's electronic information systems; (2) defining the information to be collected by applying reasonable selection criteria, including search terms, date restrictions, or folder designations; or (3) avoiding collection efforts that are disproportionate to, or are inappropriate in, the context of a particular litigation.

Discovery should not be permitted to continue indefinitely merely because a requesting party can point to undiscovered documents and electronically stored information when there is no indication that the documents or information are relevant to the case, or further discovery is disproportionate to the needs of the case.

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

RESOURCES AND AUTHORITIES

Fennell v. First Step Designs, Ltd., 83 F.3d 526, 532-33 (1st Cir. 1996) (affirming order denying electronic discovery where that discovery would be a "fishing expedition").

Comment 6.c. Rule 34 inspections

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

a) revealing trade secrets
b) revealing other highly confidential or private information, such as personnel evaluations and payroll information, properly private to individual employees
c) revealing confidential attorney-client or work-product communications
d) unreasonably disrupting the ongoing business; and
e) endangering the stability of operating systems, software applications, and electronic files if certain procedures or software are used inappropriately.

Further, Rule 34 inspections of electronically stored information are likely to be particularly ineffective. The standard form of production, in which the producing party identifies and produces responsive information, allows the party with the greatest knowledge of the computer systems to search and utilize the systems to produce responsive information. A Rule 34 inspection, in contrast, requires persons unfamiliar with the party's recordkeeping systems, hardware, and software to attempt to manipulate the systems. Not only is such a process disruptive, it is less likely to be fruitful. In most cases, producing parties will be able to argue persuasively that their production of relevant electronically stored information from computer systems and databases was sufficient to discharge their discovery obligations.

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: (1) be documented in an agreed-upon (and/or court-ordered) protocol; (2) recognize the rights of nonparties, such as employees, patients, and other entities; and (3) be narrowly restricted to protect confidential and personally identifiable information and system integrity as well as to avoid giving the discovering party access to information unrelated to the litigation. Further, no inspection should be permitted to proceed until the producing party has had a fair opportunity to review the information subject to inspection. Where the requesting party makes the required showing to justify inspection of the other party's systems, the information subject to inspection should be dealt with in such a manner as to preserve the producing party's rights and obligations, for example, through the use of "neutral" court-appointed consultants.

RESOURCES AND AUTHORITIES

In re Ford Motor Co., 345 F.3d 1315, 1317 (11th Cir. 2003) (district court abused discretion in granting *ex parte* motion to compel access to defendant's databases; noting that granting a motion to inspect the databases requires a discussion of whether the defendant failed to comply with the original discovery requests, the validity of defendant's objections to the request, and any protocols or limits needed to narrow the scope of the search).

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 electronically stored information. Due to the complexity of electronic discovery, many organizations rely on consultants to provide a variety of services, including discovery planning, data collection, specialized data processing, and forensic analysis. Such consultants can be of great assistance to parties and courts in providing technical expertise and experience with the collection, review, and production of electronically stored information. However, parties should carefully consider the experience and expertise of a potential consultant before his or her selection, as standards for experts and consultants in this field have not been fully developed. Vendors offer a variety of software and services to assist with the electronic discovery process and a party's evaluation of vendor software and services should include the defensibility of the process in the litigation context, the cost, and the experience of the vendor. Ultimate responsibility for ensuring the preservation, collection, processing, and production of electronically stored information rests with the party and its counsel, not with the nonparty consultant or vendor.

At all times, counsel, clients, and vendors must understand everyone's role in the discovery process. Thus, even if a vendor is retained to serve in a non-testifying capacity, everyone should be aware of the potential need for testimony if forensic or other technical expertise is required to prepare electronically stored information for review or production. Additionally, care should be taken to ensure that the vendor does not assume the role of a legal advisor, and that all persons involved understand what communications are protected under the attorney-client privilege and what information may be protected as attorney work product.

For an additional discussion of this issue, see *Comment 10.c. (Use of special masters and court-appointed experts to preserve privilege).*

RESOURCES AND AUTHORITIES

N.Y. Bar Ass'n Formal Op. 2006-3 (concluding that where an outsourcing assignment requires a lawyer to disclose client confidences or secrets to an overseas non-lawyer, the lawyer must secure the client's informed consent in advance and must be mindful of different laws and traditions regarding the confidentiality of client information that exist overseas).

Gates Rubber Co. v. Bando Chem. Indus., Ltd., 167 F.R.D. 90, 100 (D. Colo. 1996) (appointing special master to secure materials from alleged destruction and simultaneously protect the rights of producing party to object to the production of certain materials under the usual rules of discovery).

Comment 6.e. Documentation and validation of collection procedures for electronically stored information

In developing collection procedures *for electronically stored information*, organizations should consider the appropriate scope of the collection, the cost *of the collection, the* burden *on* and disruption of normal *business* activities, and the defensibility of the process *itself*. All collection processes should be accompanied by *documentation and validation* appropriate *to the needs of the particular case*. Well-documented collection and production procedures enable an organization to respond to challenges – even those made years later – to the collection process, to avoid overlooking *electronically stored information* that should be collected, *and to avoid collecting electronically stored information that is neither relevant nor responsive to the matter at issue.* The documentation *of the collection process* should describe what is being collected, the procedures *employed* and steps *taken to ensure the integrity of* the information collected. *Finally, this* documentation should be revised *as* the organization *introduces* new or different technology.

Comment 6.f. Role of and risks to counsel regarding the preservation and production of electronically stored information

Generally speaking, the obligation to preserve and produce discoverable electronically stored information runs to and must be executed by parties to an action. However, counsel (both inside and outside) have very practical ethical and other responsibilities to ensure that the efforts to preserve and produce electronically stored information comply with the applicable requirements. While it is generally sufficient for counsel to furnish advice to clients and rely upon them to meet their obligations, courts have suggested that counsel has independent duties of supervision and, in some cases, of participation in the preservation and production process. Under the reasoning of those decisions, counsel must supervise the implementation of preservation or collection efforts of clients.

The volume and dynamic nature of electronic information make discovery more complex and difficult. The increased risks created by these complexities require both inside and retained counsel to meet a high standard of care in regard to discovery of electronically stored information. For cases pending in the federal courts, Rule 26(f)'s early meet and confer obligations and the affirmative disclosure obligations of Rule 26(b)(2)(B) ("identification" of sources not reasonably accessible because of undue burden and cost) imply that counsel must undertake early preparation sufficiently diligent to adequately represent the parties' positions. This position is reinforced by the Committee Notes to Rule 26(f), district court local rules, and court decisions.

Similar requirements exist in state courts. For example, the Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information (Guideline 2) recommend that a judge should "encourage" counsel to become familiar with the operation of the relevant information management systems, including how information is stored and retrieved.

The enhanced possibility of inadvertent production of privileged or work product information, the stakes in the management of privilege reviews, and careless handling of client communications raise serious ethical issues. Similarly, the disparate views on how lawyers should treat metadata (e.g., when to delete, when to send, when to review) create additional risks for lawyers, especially in cases across different jurisdictions.

RESOURCES AND AUTHORITIES

D. Kan. *Guidelines for Discovery of Electronically Stored Information* (parties have a duty to discuss the preservation of electronically stored information during the Fed. R. Civ. P. 26(f) conference).

D.N.J. L. R. 26.1(d) (parties have a duty to discuss the preservation of electronically stored information during the Fed. R. Civ. P. 26(f) conference).

Gregory G. Wrobel, *et al., Counsel Beware: Preventing Spoliation of Electronic Evidence in Antitrust Litigation,* 20-SUM Antitrust 79, 80 (2006).

ABA Civil Discovery Standards (1999) (rev. Aug. 2004) *available at* http://www.abanet.org/litigation/decisionstandard/2004civildiscoverystandards.pdf (discussion of duty of counsel).

Model Rules of Prof'l Conduct R. 3.4.("A lawyer shall not unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value.").

Compare, e.g., Maryland Bar Assoc. Comm. on Ethics Op. 2007-09 (Maryland lawyers who produce electronic materials in discovery have the professional duty to take reasonable measures to avoid the disclosure of confidential information embedded in metadata within the document; lawyers who receive electronic discovery materials have no ethical duty to refrain from viewing or using metadata; recent amendments to the Federal Rules of Civil Procedure regarding electronic discovery will impact the obligations of lawyers) *with* Florida Bar Opinion 06-02, ABA Comm. on Eth. & Prof'l Resp., Formal Op. 06-422 (2006), and NYSB Opinion 749 (a lawyer has both a duty to refrain from reviewing or using metadata and a duty to notify an adversary of inadvertent production).

In re Grand Jury Investigation, 445 F.3d 266, 275 (3rd Cir. 2006), *cert. denied, Doe v. United States,* 127 S.Ct. 538 (2006) (contents of discussions not privileged when the client may be committing crime of obstruction of justice by participating in a scheme to delete emails after receiving information from counsel about scope of pending subpoena).

Metro. Opera Ass'n, Inc. v. Local 100 Hotel Employees & Rest. Employees Int'l Union, 212 F.R.D. 178, 230 (S.D.N.Y. 2003) (finding that "the combination of outrages perpetrated by the [defendant] and its counsel, by both omission and commission" warranted the most severe sanction, and entered a judgment of liability against the defendant based on, inter alia, Rule 26(g) and inherent power of the court.), adhered to in *Metro. Opera Ass'n, Inc. v. Local 100 Hotel Employees & Rest. Employees Int'l Union, No. 00 Civ. 3613*(LAP), 2004 WL 1943099, at *8-9 (S.D.N.Y. Aug. 27, 2004) (affirming that sanctions under Rule 26(g) are imposed when a competent attorney could not have believed a filing was well grounded in fact and warranted in law).

Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 432-34 (S.D.N.Y. 2004) (*"Zubulake V"*) (counsel has obligation to work with client to identify all potential sources of relevant information; party sanctioned for, destruction of documents after being told repeatedly by counsel not to do so, and counsel's failure to identify key witnesses).

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

Comment 7.a. Resolving discovery disputes

A party that receives a request for production of electronically stored information may object to some or all of the request, or may produce information that the requesting party deems inadequate or nonresponsive. This may prompt the requesting party to consider filing a motion to compel production. In cases governed by the Federal Rules, such a motion would be filed under Rule 37(a), which requires the moving party to certify that good-faith efforts have been made to resolve the dispute before resorting to the court. Fed R. Civ. P. 37 (a)(2)(A).

On a motion to compel, the moving party must demonstrate that the producing party's response to the discovery request, including its steps to preserve and produce electronically stored information, was inadequate, and that additional efforts are warranted. In so doing, a court should consider the balancing principles of Sedona Principle 2 and the proportionality limits of Rule 26(b)(2)(C), especially with respect to the technological feasibility and realistic costs of preserving, retrieving, producing, and reviewing electronically stored information.

Rule 26(b)(2)(B) establishes a procedure to resolve disputes regarding discovery from sources the responding party has identified as "not reasonably accessible" because of "undue burden or cost." This is discussed at Comment 2.c. Rule 26(c) establishes a procedure for obtaining a protective order to relieve a responding party from "undue burden or expense." Under either rule, the burden is on the responding party to establish the grounds for limiting discovery.

RESOURCES AND AUTHORITIES

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), *available at* http://www.uscourts.gov/rules/reports/st90-2005.pdf.

Comment 7.b. Discovery from non-parties

Electronically stored information may also be secured from nonparties by service of a subpoena or other process authorized by the relevant court procedures. Requesting parties must be sensitive to the burdens that such discovery places on nonparties.

In cases governed by the Federal Rules, Rule 45 has been explicitly extended to include electronically stored information within the scope of the types of information the inspection or production of which may be demanded. A party issuing the subpoena may indicate the form or forms in which production is to be made and the nonparty subject to the subpoena has the same rights and obligations in regard to production as parties. One major exception, of course, is that there is no mandatory discussion, prior to discovery, of a discovery plan or the opportunity to meet and discuss preservation or other key topics. The intent of the Advisory Committee was that parties issuing and responding to subpoenas would avail themselves of such an opportunity informally, a best practice that should be followed in most cases.

Under a 1991 amendment to the Federal Rules of Civil Procedure, Rule 45(c)(1) added a requirement not generally available to party litigants to the effect that the issuing party must "take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena." Equally important, Rule 45(c)(2)(B) provides that, if objection is made to a subpoena, "an order to compel production *shall protect* any person who is not a party or an officer of a party from significant expense resulting from the inspection and copying commanded." (Emphasis supplied).

Courts balance the cost, burden, and need for discovery from nonparties when considering whether to quash or modify the discovery sought, or to shift some or all of the costs associated with requests for production of electronically stored information. (For cost-shifting standards on non-party subpoenas, *see* Comment 13.c.).

Excessively broad electronic document production requests directed to third parties can also lead to sanctions under Rule 45 and to liability under federal statutes protecting the privacy of electronic communications. As a result, requesting parties must carefully tailor requests directed to nonparties and should undertake efforts to negotiate with them the scope of the electronically stored information requested and the manner of production.

RESOURCES AND AUTHORITIES

Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure,* 4 Nw. J.Tech. & Intell. Prop. 171, 205 (2006) *available at* http://www.law.northwestern.edu/journals/njtip/v4/n2/3.

Nicholas v. Wyndham Int'l., Inc., 373 F.3d 537, 543 (4th Cir. 2004). ("District court's denial of discovery from nonparty [corporation owned by plaintiffs], which was sought in ancillary proceeding by defendant in underlying proceeding pending in district outside the instant circuit, was immediately appealable, under collateral order doctrine, since review of denial would not be available via either appeal or contempt proceedings." However, court denied the defendant's request for discovery from non-party corporation owned by plaintiffs where plaintiffs had already been deposed and produced more than 400 pages of emails, including some from their corporation's account, and defendant's counsel conceded to the district court that non-party corporation "could have no more information about the facts of liability and damages than Plaintiffs themselves had.").

Theofel v. Farey-Jones, 341 F.3d 978 (9th Cir. 2003), amended, 359 F.3d 1066, 1073-74 (9th Cir. 2004) (holding that service of an overbroad, "patently unlawful" subpoena on a party's ISP, which led to the disclosure of private and privileged communications, violated the Stored Communications Act 18 U.S.C. § 2701(a) (2004), which provides a cause of action against anyone who intentionally accesses without authorization a facility through which an electronic communication service is provided or intentionally exceeds an authorization to access that facility and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage. 18 U.S.C. § 1030(a)(2)(C) (2004) provides a cause of action against one who intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer if the conduct involved any interstate or foreign communication, 18 U.S.C. § 2701 *et seq.,* and the Computer Fraud and Abuse Act, U.S.C. § 1030 (2004).

8. The primary source of electronically stored information for production should be active data and information. Resort to disaster recovery backup tapes and other sources of electronically stored information that are not reasonably accessible requires the requesting party to demonstrate need and relevance that outweigh the costs and burdens of retrieving and processing the electronically stored information from such sources, including the disruption of business and information management activities.

Comment 8.a. Scope of search for active and purposely stored data

The scope of a search for relevant electronically stored information must be reasonable. For example, potentially relevant information may be located or reside on local and network computers, laptop computers, servers, handheld or portable storage devices (such as PDAs and flash memory drives), archive and backup data tapes, cellular phones, voicemail systems, or closed-circuit television monitoring systems.

However, it is neither feasible nor reasonable to require that litigants immediately or always canvas all potential reservoirs of electronically stored information in responding to preservation obligations and discovery requests. Many locations or sources will contain duplicative or redundant information, 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, about the active and purposely stored data locations that should be subject to preservation efforts. If the producing party is aware (or reasonably should be aware) that specific relevant information can only be obtained from a particular source, that information or the source on which it is located should be preserved for possible production absent agreement of the parties or order of the court. The mere suspicion that a source may contain potentially relevant information is not sufficient to demand the preservation of that source "just in case." Rather, the appropriate standard should be to preserve information on and search sources where the producing party is reasonably likely to locate potentially relevant information not available from other available, searched sources.

Resorting to sources that are not reasonably accessible, while certainly possible under some circumstances, should be required only on a showing of good cause, with the requesting party bearing the burden to show good cause on a motion to compel or in a hearing on a protective order. Production from such less accessible sources is subject to meeting the balancing or proportionality standards set forth in Principle 2, *supra*.

> *Illustration i.* A party seeking relevant emails demands a search of backup tapes and hard drives for deleted materials. No showing of special need or justification is made for the search. The request should be denied. Parties are not typically required to sequester and search the trash bin outside an office building after commencement of litigation; neither should they be required to preserve and produce deleted electronic information in the normal case. Production should primarily be from sources of active information which is arranged in a manner conducive to retrieval and storage.
>
> *Illustration ii.* After a key employee leaves X Company ("X Co.") to work for a competitor, a suspiciously similar competitive product suddenly emerges from the new company. X Co. produces credible testimony that the former employee bragged about sending confidential design specifications to his new company computer, copying the data to a CD, and deleting the data so that the evidence would never be found. The court properly orders that, given the circumstances of the case, the requesting party has demonstrated the need for the computer to be produced for mirror image copying of its hard drive. If the defendant is not willing to undertake the expense of hiring its own reputable data recovery expert to produce all available relevant data, inspection of the computer's contents by an expert working on behalf of X Co. may be justified, subject to appropriate orders to preserve privacy, to protect data, and to prevent production of unrelated or privileged material. Under a showing of special need, with appropriate orders of protection, extraordinary efforts to restore electronic information could also be ordered.

For a discussion of the limitations under the 2006 Amendments on initial discovery from sources that are not reasonably accessible because of undue burden or cost, see *Comment 8.b.*

RESOURCES AND AUTHORITIES

Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information,* Guideline 5 (Aug. 2006) (judges should first assess if the electronically stored information is discoverable and then balance the benefits and burdens of requiring discovery based on a multi-factor analysis rather than presumptions regarding accessible or active data).

ABA Civil Discovery Standards (1999) (rev. Aug. 2004) Standard 29(b)(iv) *available at* http://www.abanet.org/litigation/discoverystandards/2004civildiscoverystandards.pdf (listing factors for a court to consider in deciding whether to limit discovery of Electronically Stored Information and allocate costs).

Comment 8.b. Production from sources that are not reasonably accessible

The 2006 Amendments to the Federal Rules limit the obligation to search and produce from sources of relevant electronically stored information that is not reasonably accessible due to undue burden or cost. This limitation in Fed. R. Civ. P. 26(b)(2)(B) is a specific invocation of the proportionality rules embodied in Rule 26(b)(2)(C).

Whether a source is "reasonably accessible" does not solely depend on the technology required to access that information, but is more closely related to the costs and burdens involved in accessing and retrieving the information. The Advisory Committee gives, as examples from current technology, "backup tapes" intended for disaster recovery purposes that are often not indexed, organized, or susceptible to electronic searching; legacy data that remains from obsolete systems and is unintelligible on the successor systems; data that was "deleted" but remains in fragmented form requiring a modern version of forensics to restore and retrieve; and databases that were designed to create certain information in certain ways and that cannot readily create very different kinds or forms of information.

The "accessibility" limitation is similar to but different from the production limitation found in Principle 8, which also addresses the technical accessibility and the purpose of the storage, rather than simply the burdens and costs associated with access.

Rule 26(b)(2)(B) of the amended Federal Rules requires the producing party to identify by category or type any sources of relevant electronically stored information that it has identified as "not reasonably accessible." Specifically, this requires that if a party has determined that the only source of some relevant electronically stored information is one that is not reasonably accessible, then it must preserve that source, disclose it (with enough information so the other side can understand what is at issue), be ready to demonstrate why production of information is unduly burdensome or expensive, and, if possible, discuss these issues at the initial Rule 26(f) meet and confer sessions. This requirement should not be read as a mandate to list all sources of electronically stored information that are not searched, nor does it require a listing of such sources if a party has reasonably determined, in good faith, that the inaccessible source does not contain nonduplicative relevant information. However, a party may not deliberately make information inaccessible for the sole purpose of avoiding litigation discovery requests specific to a known case.

If the parties are unable to reach agreement as to the accessibility of specific sources of electronically stored information or the need to restore those sources for purposes of the dispute at issue, a motion to compel or for a protective order may be brought. This procedure is discussed in Comment 2.c.

For discussion of the use of cost-shifting in electronic discovery, see *Principle 13,* infra.

RESOURCES AND AUTHORITIES

Report of the Civil Rules Advisory Committee May 27, 2005 (rev. July 25, 2005), C. 42, *available at* http://www.uscourts.gov/rules/reports/st09-2005.pdf. ("[t]he rule requires that the information identified as not reasonably accessible must be difficult to access by the producing party for all purposes, not for a particular litigation. A party that makes information 'inaccessible' because it is likely to be discoverable in litigation is subject to sanctions now and would still be subject to sanctions under the proposed rule changes.").

Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2008.2 (2d ed. 2006).

Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information, Guideline 1(a)* (Aug. 2006) (defining "accessible" information as "electronically-stored information that is easily retrievable in the ordinary course of business without undue cost and burden").

Thomas Y. Allman, *The Impact of the Proposed Federal E-Discovery Rules,* 12 Rich. J.L. & Tech. 13 (2006).

Hon. Anthony J. Battaglia, *Dealing with Electronically Stored Information: Preservation, Production, and Privilege,* 53 Fed. Law. 26 (May 2006).

Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure,* 4 Nw. J. Tech. & Intell. Prop. 171 (2006), *available at* http://www..law.northwestern.edu/journals/njtip/v4/n2/3.

Tex. R. Civ. P. 194.6 ("[T]he requesting party must specifically request production of electronic or magnetic data and specify the form in which the requesting party wants it produced. 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.").

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 319-20 n.61 (S.D.N.Y. 2003) (*"Zubulake I"*) (noting that consideration of cost-shifting is appropriate where stored data is not in a "readily usable" format, such as backup tapes; noting that Sedona Principles 8 and 9 recognize the distinction between "active data" and backup tapes in a manner very similar to the test employed in the instant case).

Comment 8.c. Forensic data collection

Intrusive access to desktop, server, laptop or other hard drives or media storage devices is sometimes ordered when key employees leave employment under suspicious circumstances, or if theft or misappropriation of trade secrets or confidential information may be involved. However, making forensic image backups of computers is only the first step of an expensive, complex, and difficult process of data analysis that can divert litigation into side issues and satellite disputes involving the interpretation of potentially ambiguous forensic evidence. While such an approach is clearly appropriate in some circumstances, it should not be required unless exceptional circumstances warrant the extraordinary cost and burden. When ordered, it should be accompanied by an appropriate protocol or other protective measures that take into account privacy rights, attorney-client privilege, and the need to separate out and ignore nonrelevant information. In some cases, it may be necessary, as an anticipatory matter, to meet certain preservation obligations by making or retaining copies of backup tapes or taking such steps as imaging the computer hard drives of departing employees, if appropriate. Such copies may best preserve all possibly relevant data. If the parties anticipate such a need, the topic of forensic-level preservation and review should be addressed at the initial meet and confer sessions.

The 2006 amendments to the Federal Rules clarify that the right to test, sample or inspect electronically stored information or gain access to computer systems or hard drives is within the scope of a discovery request, but is subject to protection from undue intrusiveness and with due respect for burdens and issues of confidentiality and privacy.

RESOURCES AND AUTHORITIES

Report of the Civil Rules Advisory Committee, May 27, 2005 (rev. July 25, 2005), *available at* http://www.uscourts.gov/rules/reports/st09-2005.pdf.

In re Ford Motor Co., 345 F.3d 1315, 1317 (11th Cir. 2003) (granting mandamus to prevent implementation of district court order allowing inspection of databases as an abuse of discretion).

McPeek v. Ashcroft, 212 F.R.D., 33, 36 (D.D.C. 2003) (declining to order searches of backup tapes where plaintiff had not demonstrated a likelihood of obtaining relevant information).

Comment 8.d. Outsourcing vendors and non-party custodians of data

The scope of discovery and the duty to preserve and produce information extend to relevant electronically stored information under the custody and control of a party, including information that a nonparty such as an information technology service provider or data processing contractor may possess. Many organizations outsource all or part of their information technology systems or share data with third parties for processing or for other business purposes. In contracting for such services, organizations should consider how they will comply with their obligations to preserve and collect electronic data for litigation. If such provisions are not within the scope of contractual agreements, costs may escalate and necessary services, including access to relevant data, may be unavailable when needed. Organizations also need to consider whether notice should be sent to nonparties, such as contractors and vendors, when litigation commences, particularly because such nonparties may not otherwise be aware of litigation or attendant preservation obligations.

RESOURCES AND AUTHORITIES

Keir v. UnumProvident Corp., No. 02 Civ. 8781, 2003 WL 21997747, at *12-13 (S.D.N.Y. Aug. 22, 2003) (finding that defendant's failure to timely notify its IT vendor of preservation order contributed to loss of responsive 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 electronically stored information.

Comment 9.a. The scope of discovery of electronically stored information

At the outset of litigation parties should consider the potential need for preservation and production of electronically stored information that is not readily apparent to ordinary employees and records custodians and be prepared to discuss the matter at the initial meet and confer session. Such information includes system data as well as deleted, shadowed, fragmented, or residual information. A party seeking such information should articulate good cause for such preservation and production. The producing party should have a good understanding of the available electronically stored information and be able to argue the costs and burdens in the context of the case, including the relevance (and lack thereof) of the information to the claims and defenses in the case. In framing these positions, both sides should also consider the potential value of such information to the usability of any production separate and apart from the substantive relevance of the contents to the merits.

> *Illustration i.* Plaintiff claims that she is entitled to a commission on a transaction, based upon an email allegedly sent by the president of defendant corporation agreeing to the commission. Defendant asserts that there is no record of the email being sent in its email system or the logs of its Internet activity, and that the email is not authentic. In these circumstances, it is appropriate to require production of not only the content of the questioned email, but also of the email header information and metadata, which can play a crucial role in determining whether the questioned message is authentic.
>
> *Illustration ii.* Plaintiff alleges that the defendant engaged in billing fraud by overcharging for hourly work done for another client. The plaintiff presents two copies of an invoice indicating material differences. In this case, discovery of overwritten drafts, edits and deleted versions of the invoices may be appropriate.

RESOURCES AND AUTHORITIES

Concord Boat Corp. v. Brunswick Corp., No. LR-C-95-781, 1997 WL 33352759, at *9 (E.D. Ark. Aug. 29, 1997) ("Fourteen days worth of email, which might contain a few deleted emails, 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 [ ] email.").

McPeek v. Ashcroft, 202 F.R.D. 31, 33 (D.D.C. 2001) (rejecting notion that there is an absolute obligation to pursue potentially relevant data on backup tapes absent specific reason to do so).

Comment 9.b. Deleted electronically stored information

Deleted information may at one time have been a "useful" document generated in the ordinary course of business that had value to the organization, although that value may have expired. However, this historic fact alone does not justify the retrieval and review of deleted information. Case law indicates that only exceptional cases turn on "deleted" or "discarded" information (whether paper or electronic). Employees and organizations properly and routinely delete or destroy documents and electronically stored information that no longer have business value, so long as the information was not subject to regulatory, investigatory, or litigation preservation obligations when deleted or destroyed.

Accordingly, as a general rule and absent specific circumstances, organizations should not be required to preserve deleted electronically stored information in connection with litigation. While most computer systems will have a plethora of deleted information that could in theory be "mined," there should not be a routine obligation for such preservation and discovery. If, as usual, deleted information is not accessed by employees in the ordinary course of business, there is presumptively no reason to require the routine preservation of such information. The relevance will, at best, be marginal in most cases, while the burdens involved will usually be great. In exceptional cases, however, there may be good cause for targeted preservation of deleted and residual data.

Parties should communicate early about the possible relevance of deleted electronically stored information in order to avoid costly and unnecessary preservation, on one hand, or claims of spoliation, on the other.

For a related discussion of form or forms of production, including the preferred process for reaching agreement on these topics, see *generally Principle 12,* infra. *For a more specific discussion of forensic collection,* see *Principle 8 at Comment 8.c.*

RESOURCES AND AUTHORITIES

Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2008.2 (2d ed. 2006).

Tex. 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.").

Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?,* 41 B.C. L. Rev. 327, 372 (2000) (Under former Rule 34(a), "[e]mbedded 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'.").

10. A responding party should follow reasonable procedures to protect privileges and objections in connection with the production of electronically stored information.

Comment 10.a. Potential waiver of confidentiality and privilege in production and the use of "clawback" agreements and procedures.

Because of the large volumes typically involved when electronically stored information is produced, parties should consider entering into agreements among themselves, including nonwaiver agreements, which outline the procedures to be followed to protect against any waiver of privileges or work product protection due to the inadvertent production of documents and data. Notably, the validity and impact of such nonwaiver agreements as to nonparties may vary greatly among jurisdictions. Similarly, the ethical obligations of counsel may vary. These nonwaiver agreements typically provide for the sequestering, return and/or destruction of the inadvertently produced information. Such agreement may include "clawback" arrangements that allow the producing party to "claw back" or "undo" the production. (As noted below, a "clawback" agreement is substantively different from a "quick peek" agreement. *See* Comment 10.d).

Counsel should discuss the need for such a provision at the outset of litigation and should approach the court for entry of an appropriate nonwaiver order. Under the 2006 Amendments, the discussions should take place at the Rule 26(f) conference and counsel can use Form 35 for inclusion in the Rule 16(b) Scheduling Order.

If an order is entered by a court endorsing the approach selected, the order should provide that the inadvertent disclosure of a privileged or work product document does not constitute a waiver of privilege, that the privileged document should be returned (or certification that it has been deleted), and that any notes or copies discussing the privileged or work product information will be destroyed or deleted.

The 2006 Amendments to the Federal Rules provide for a procedure whereby a claim of inadvertent production of privileged information or work product material can be made and the receiving party is obligated to sequester, destroy, or return the allegedly privileged information, or sequester it pending a court hearing. Fed. R. Civ. P. 26(b)(5). It is important to note that Rule 26(b)(5)(B) only provides the procedure for dealing with claims of inadvertent production and does not provide guidance regarding the substantive privilege law, including whether the inadvertent production results in waiver.

RESOURCES AND AUTHORITIES

Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information,* Guideline 4(D) (Aug. 2006) (parties should discuss procedures to be used if privileged electronically stored information is inadvertently disclosed); Guideline 8 (setting forth recommended factors for a court to use in determining if a party has waived the privilege because of an inadvertent disclosure).

ABA Civil Discovery Standard (1999)(rev. Aug. 2004) Standard 32(a), (c) and (e), *available at* http://www.abanet.org/litigaton/discoverystandards/2004civildiscoverystandards.pdf.

Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2016.3 (2d ed. 2006).

John M. Facciola, *Sailing on Confused Seas: Privilege Waiver and The New Federal Rules of Civil Procedure,* 2006 Fed. Cts. L. Rev. 6 (2006).

Joseph L. Paller Jr., *Gentlemen Do No Read Each Other's Mail: A Lawyer's Duties Upon Receipt of Inadvertently Disclosed Confidential Information,* 21 Lab. Law. 247 (Winter/Spring 2006).

Denis R. Kike, *Waiving the Privilege in a Storm of Data: An Argument for Uniformity and Rationality In Dealing with the Inadvertent Production of Privileged Materials in the Age of Electronically Stored Information,* 12 Rich. J.L. & Tech. 15 (2005).

John K. Villa, *The Inadvertent Disclosure of Privileged Material: What is the Effect on the Privilege and the Duty of Receiving Counsel?* 22 No. 9 ACC Docket 108 (Oct. 2004).

Jonathan M. Redgrave & Kristin M. Nimsger, *Electronic Discovery and Inadvertent Productions of Privileged Documents,* 49 Fed. Law. 37 (July 2002).

In re Qwest Communications Int'l, Inc. Sec. Litig., 450 F.3d 1179, 1200 (10th Cir. 2006) (refusing mandamus request regarding the order compelling disclosure in discovery of information furnished to government because of waiver of privilege; refusing to recognize "selective" waiver concept).

Hopson v. Mayor and City Council of Baltimore, 232 F.R.D. 228, 239-41 (D. Md. 2005) (arguing that risks of inadvertent waiver can be mitigated through use of scheduling orders, protective orders or discovery management orders agreed to by the parties and determined reasonable by the courts that protect produced documents from waiver; court further notes that such agreements will not excuse parties from making reasonable pre-production efforts to protect privileged material and recommends parties assume complete pre-production privilege review as required unless such review can be shown with particularity to be unduly burdensome or expensive).

Comment 10.b. Protection of confidentiality and privilege regarding direct access to electronically stored information or systems

Special issues may arise with any request to secure direct access to electronically stored information or to computer devices or systems on which it resides. Protective orders should be in place to guard against any release of proprietary, confidential, or personal electronically stored information accessible to the adversary or its expert.

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

The 2006 Amendments to Rule 34(a) clarify that the right to "test or sample," as well as the right to "inspect," extends to both electronically stored information and the system on which it is stored. The Committee Note makes it clear, however, that this change is "not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. The Note further states that the inspection or testing "may raise issues of confidentiality or privacy" and mandates that "[c]ourts should guard against undue intrusiveness resulting from inspecting or testing such systems." Fed. R. Civ. P. 34 Committee Note (2006).

The 2006 amendments also permit, but do not require or provide for a court to order, that a party may make available business records in the form of electronically stored information to enable an opponent to derive an interrogatory answer in lieu of the party answering. Fed. R. Civ. P. 33(d). The Committee Note restricts this option to situations in which the burden of deriving an answer is substantially the same for either party. The party electing to respond by referencing electronically stored information must do so in a way that allows the interrogating party to locate and identify the information as "readily as can the party served." The Note goes on to say that in some circumstances the ability to satisfy these circumstances may require the responding party to provide technical support, information on application software, or other assistance. In fact, the Note specifically cautions that if necessary to afford the requesting party an adequate opportunity to derive or ascertain the answer to the interrogatory, the party electing to reference electronically stored information "may be required to provide direct access to its electronic information system." Fed. R. Civ. P. 33(d) Committee Note (2006).

Because of the risk of unintended costs and opening IT infrastructures to opposing parties, parties and counsel should carefully consider if and when they will elect to refer to a production of electronically stored information in a Rule 33(d) election rather than providing a substantive response to the interrogatory. Indeed, the Committee Note to the Rule acknowledges that because of "the responding party's need to protect sensitive interests of confidentiality or privacy," the party may choose to derive the answer itself rather than invoke Rule 33(d).

RESOURCES AND AUTHORITIES

In re Ford Motor Co., 345 F.3d 1315, 1317 (11th Cir. 2003) (granting mandamus to prevent implementation of district court order allowing inspection of databases as an abuse of discretion).

Comment 10.c. Use of special masters and court-appointed experts to preserve privilege

In certain circumstances, a court may find it beneficial to appoint a "neutral" person (e.g., a special master or court-appointed expert) who can help mediate or manage electronic discovery issues. The December 1, 2003 amendment to Rule 53 (Special Masters) clarifies that special masters are available to federal courts to address electronic discovery issues in appropriate cases where the matters cannot be addressed effectively and timely by an available district or magistrate judge. *See* Fed. R. Civ. P. 53(a)(1)(C).

Using a court-appointed "neutral" person to mediate electronic discovery issues may prove beneficial for a number of reasons. First, using such a person to mediate disputes and, if necessary, conduct initial inspections of any disputed documents, generally eliminates any privilege-waiver concerns regarding such inspections. Second, the "neutral" person may be able to speed the resolution of disputes by fashioning fair and reasonable discovery plans based upon specialized knowledge of electronic discovery and/or technical issues in light of specific facts in the case. *See id.*

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

RESOURCES AND AUTHORITIES

Shira A. Scheindlin and Jonathan M. Redgrave, *Revisions in Federal Rule 53 Provide New Options for Using Special Masters in Litigation,* 76 New York State Bar J. 18 (Jan. 2004).

Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050, 1055 (S.D. Cal. 1999) (use of computer specialist was appropriate to review hard drive for relevant data, and no view of privileged material by specialist would constitute waiver of privilege).

Comment 10.d. Protection of confidentiality and privilege regarding "quick peek" agreements

Given the enormous volume of electronic documents generated and retained in today's business environment, and in light of the demands of litigation, there is an increasing interest in production under a "quick peek" agreement to protect against waiver of confidentiality and privilege.

In a "quick peek" production, documents and electronically stored information are produced to the opposing party before being reviewed for privilege, confidentiality, or privacy. Such a production requires stringent guidelines and restrictions to prevent the waiver of confidentiality and privilege. Under a "quick peek" agreement, if the requesting party selects a document that appears to be privileged, the producing party can identify the document as privileged and withdraw it from production without having waived any privilege.

A "quick peek" procedure or order should not be lightly entered and requires the voluntary consent of the producing party. While providing the advantage of reducing the costs of preproduction reviews for privilege and confidentiality (and maybe even responsiveness), there are potential risks and problems that should be carefully considered.

First, the voluntary production of privileged and confidential materials to one's adversary, even in a restricted setting, is inconsistent with the tenets of privilege law that, while varying among jurisdictions, usually require the producing party to meticulously guard against the loss of secrecy for such materials. The fact that an adversary sees the voluntarily produced document in any circumstance arguably serves as a waiver or loss of privilege or protection.

Second, despite the strongest possible language in any "quick peek" order to protect against waiver of privileges, there is currently no effective way to extend the scope of the order to restrict persons who are non-parties to the agreement from seeking the production of privileged materials that have been produced under such an order. For example, parties in mass tort and product liability cases, who are subject to multiple suits by different counsel in different states, face the risk that their "quick peek" agreement entered in one action may not protect the party from waiver arguments in other actions, even if they have a strong protective order in the first action. Given the differences in privilege laws among jurisdictions, this uncertainty presents a serious and legitimate impediment to any widespread acceptance of a "quick peek." While the proposed Rule of Evidence 502 being discussed by the Advisory Committee may eventually result in a uniform federal and state approach to issues relating to such agreements on waiver, this is not the current situation.

Third, counsel have an ethical duty to guard zealously the confidences and secrets of their clients. It is possible that questions could arise as to whether voluntarily entering into a "quick peek" production could constitute a violation of Model Rule of Prof'l. Conduct R. 1.1 (2002)(requiring a lawyer to use diligence and care in representation) or Model Rule of Prof'l. Conduct R.1.6 (2002) (protection of client secrets and confidences) if the manner of the production results in later waivers of privileges and protections. While this may seem unlikely, it has already arisen in the context of inadvertent productions. D.C. Bar Ethics Opinion 256 (1995) (examining whether actions of producing counsel violated standard).

Fourth, the genie cannot be put back in the lamp. The disclosure of privileged communications and work product to an adversary can adversely affect the client's interest, notwithstanding non-waiver provisions.

Fifth, there are a host of issues regarding the possible privacy rights of employees and nonparties that may be implicated in a voluntary "quick peek" production. Careful consideration should be given to a company's privacy commitments to employees and customers, its contractual privacy agreements with nonparties, and judicial process exceptions within the applicable privacy laws or regulations before a party enters into a "quick peek" agreement.

Accordingly, given the possible loss of privilege and property rights that could accompany a waiver determination, courts should not compel use of a "quick peek" procedure over the objection of a producing party. Even when large volumes of electronic documents are involved, parties are well-advised to search for privileged documents.

In those very limited instances in which a "quick peek" order may be practicable and in the parties' interests (as reflected by voluntary consent), the court should enter an order that: (1) indicates that the court is compelling the manner of production; (2) states such production does not result in an express or implied waiver of any privilege or protection for the produced documents or any other documents; (3) directs that the reviewing party cannot discuss the contents of the documents or take any notes during the review process; (4) permits the reviewing party to select those documents that it believes are relevant to the case; and (5) orders that for each selected document, the producing party either (a) produces the selected document, (b) places the selected document on a privilege log, or (c) places the selected document on a non responsive log (i.e., regardless of the privileged status, the document is not relevant to the litigation.).

RESOURCES AND AUTHORITIES

Conference of Chief Justices, *Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Information,* Guideline 4(D) (Aug. 2006) (advocating agreement for process to be used if privileged electronically stored information is inadvertently disclosed); Guideline 8 (setting forth recommended factors for a court to use in determining if a party has waived the privilege because of an inadvertent disclosure).

Report of the Advisory Committee on Evidence Rules, Proposed Rule 502(b) (June 30, 2006) *available at* http://www.aspenlawschoo.com/books/mueller_evidence/updates/excerp_ev_report_pub.pdf.

Charles Alan Wright, Arthur R. Miller, & Richard L. Marcus, *Federal Practice and Procedure* § 2016.3 (2d ed. 2006).

Kenneth S. Broun & Daniel J. Capra, *Getting Control of Waiver of Privilege in the Federal Courts: A Proposal for a Federal Rule of Evidence 502,* 58 S.C. L. Rev. 211 (2006).

John M. Facciola, *Sailing on Confused Seas: Privilege Waiver and the New Federal Rules of Civil Procedure,* 2006 Fed. Cts. L. Rev. 6 (2006).

Shira A. Scheindlin and Jonathan M. Redgrave, *Discovery of Electronic Information, in 2 Bus. & Commercial Litig. in Fed. Courts,* Ch 22 (Robert L. Haig ed. 2005 & Supp. 2006).

ABA Civil Discovery Standards (1999) (rev. Aug. 2004), Standard 32(d)(ii) and (f), *available at* http://www.abanet.org/litigaton/discoverystandards/2004civildiscoverystandards.pdf..

Transamerica Computer v. IBM, 573 F.2d 646, 651 (9th Cir. 1978) (finding no waiver of privilege when IBM produced privileged information without intending to waive privilege under "accelerated discovery proceedings [which] [i]imposed such incredible burdens on IBM" that they were "in a very practical way" compelled to produce privileged documents).

Hopson v. The Mayor and City Council of Baltimore, 232 F.R.D. 238 (D. Md. 2005) (reviewing the law of privilege waiver and the effect of clawback agreements, and formulating an order most likely to withstand anticipated challenges).

Murphy Oil USA, Inc. v. Fluor Daniel, Inc., No. Civ. A. 99-3564, 2002 WL 246439, at *7 (E.D. La. Feb. 19, 2002) (noting that court cannot compel the disclosure of privileged communications in clawback arrangement).

Comment 10.e. Privacy, trade secret, and other confidentiality concerns

Electronic information systems contain significant amounts of information that may be subject to trade secret, confidentiality, or privacy considerations. Examples of such information include proprietary business information such as formularies, business methods, sales strategies, marketing and forecasting projections, and customer and employee personal data (e.g., social security and credit card numbers, employee and patient health data, and customer financial records).

Privacy rights related to personal data may extend to customers, employees, and non-parties. Although the identification and protection of privacy rights are not directly addressed in the 2006 amendments, ample protection for such information during discovery is available through a Rule 26(c) protective order or by party agreement. In negotiating protections for such information, a party should consider the scope of the applicable privacy rights, as defined in the operative contract or rule of law, including whether such scope includes a judicial process exception. When potential discovery of documents or electronically stored information located outside of the United States is involved, the parties should pay specific attention to the foreign privacy or blocking statutes, for example, the Data Protection Act enacted by the European Union.

See also Comment 10b, *supra*, dealing with the confidentiality, privacy and privilege issues implicated under amended Rules 33(d) and 34(a) of the Federal Rules when direct access to business records are made available voluntarily or when a court is requested to order testing, sampling or inspection of electronically stored information or the information systems on which it resides.

RESOURCES AND AUTHORITIES

The Sedona Guidelines on Confidentiality and Public Access (2007), available at http://www.thesedonaconference.org.

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

Comment 11.a. Search method

In many cases, electronically stored information is found in broad groupings based on the "container" and not the "content," such as an email "inbox" or "outbox," or on a shared drive, or on a web server. In many instances, such unstructured or semi-structured data is not archived in a manner that can be used to readily identify relevant information.

Because of the enormous volume of information involved, as well as the cost and time savings made possible by technology, it is often advisable, if not necessary, to use technology tools to help search for, retrieve, and produce relevant information. For example, selective use of keyword searches can be a reasonable approach when dealing with large amounts of electronic data. Examples of search terms include the names of key personnel, date ranges, and terminology related to a specific event. It is also possible to use technology to search for "concepts," which can be based on ontologies, taxonomies, or data clustering approaches, for example.

Organizations should internally address search terms and other filtering criteria as soon as possible so that they can begin a dialogue on search methods as early as the initial discovery conference. Parties should understand the use of search methods may involve an iterative approach with search terms and concepts subject to expansion or refinement as the case progresses. Absent an agreement on the search methods to be used, parties should expect that their choice of search methods will need to be explained, either formally or informally, in subsequent legal contexts, including in depositions, evidentiary proceedings, and possibly even at trial.

> *Illustration i.* The relevant custodians each have 2 GB of information on their hard drives. Rather than read every file, the producing party reaches agreement with the requesting party on a series of search terms that capture the key concepts in the allegations of the complaint, combined with restrictions for the relevant time frame, to identify potentially responsive information. The party then reviews this subset to produce (or log) the relevant documents. The producing party has satisfied its search obligations.

Courts should encourage and promote the use of search and retrieval techniques in appropriate circumstances. For example, use of search terms could reveal that a very low percentage of files (such as emails and attachments) on a data tape contain terms that are responsive to "key" terms. This may weigh heavily against a need to further search that source, or it may be a factor in a cost-shifting analysis. Such techniques may also reveal substantial redundancy between sources (i.e., duplicate data is found in both locations) such that it is reasonable for the organization to preserve and produce data from only one of the sources. *See* Comment 11.c., *infra*.

Ideally, the parties should agree on the search methods, including search terms or concepts, to be used as early as practicable. Such agreement should take account of the iterative nature of the discovery process and allow for refinement as the parties' understanding of the relevant issues develops. The search terms employed must be reasonably calculated to yield relevant data. If not, courts may need to order additional searches, which will increase the cost and burden of discovery.

RESOURCES AND AUTHORITIES

Steven C. Bennett, *E-Discovery by Keyword Search,* 15 No. 3 Prac. Litigator 7 (2004).

George L. Paul and Jason R. Baron, *Information Inflation: Can the Legal System Adapt?* 13 Rich. J.L. & Tech. 10 (2007) *available at* http://law.richmond.edu/jolt/v13i3/article10.pdf.

Treppel v. Biovail Corp., 233 F.R.D. 363, 374 (S.D.N.Y. 2006) (stating that requesting party's refusal to agree upon identification of custodians or search terms to be applied to electronically stored information was a "missed opportunity," but did not excuse responding party's obligation to locate and produce responsive documents).

Zubulake v. UBS Warburg LLC, No. 229 F.R.D. 422, at *7-8 (S.D.N.Y. July 20, 2004) (*"Zubulake V"*) faulting counsel for failing to interview key players in litigation or do key-word search of databases in course of creating and enforcing litigation hold).

Comment 11.b. Sampling

Parties should consider the use of sampling techniques, when appropriate, to narrow the burden of searching voluminous electronically stored information. By reviewing an appropriate sample of a large body of electronically stored information, parties can often determine the likelihood that a more comprehensive review of the materials will yield useful information.

For example, in the seminal case of *McPeek v. Ashcroft,* 202 F.R.D. 31 (D.D.C. 2001), Magistrate Judge Facciola ordered the "backup restoration of the emails attributable to" a particular individual's computer during a one-year period. Judge Facciola viewed this restoration as "a test run," which would allow the court and the parties to better determine whether a further search of the backup tapes was justified. Upon reviewing the results of the sample restoration, Judge Facciola held that further restoration of backup tapes was largely unjustified and ordered very limited discovery of emails contained on backup tapes. *Id.* at 34.

Fed. R. Civ. P34(a) expressly permits sampling of electronically stored information. In ruling on a party's request to inspect computer systems, the court must consider issues of burden and intrusiveness.

RESOURCES AND AUTHORITIES

McPeek v. Ashcroft, 202 F.R.D. 31, 34-35 (D.D.C. 2001) (in sexual harassment case where plaintiff sought restoration and searches of extensive archived emails, magistrate judge ordered a "test run" search of one individual's email from a one-year period, observing that the results would dictate the need for further searches).

McPeek v. Ashcroft, 212 F.R.D. 33, 34 (D.D.C. 2003) (discussing results of previously ordered "test run" searches and concluding that further restoration of backup tapes not warranted).

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 324 (S.D.N.Y. 2003) (*"Zubulake I"*)("Requiring the responding party to restore and produce responsive documents from a small sample of backup tapes will inform the cost-shifting analysis.").

Comment 11.c. Consistency of manual and automated collection procedures

Depending on the nature of the sources of data, 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 is performed by the document authors or custodians themselves, by litigation support or information services personnel, or by others. In a manual collection, the items may be copied or transmitted by the end-user. This should be accomplished under a defined written protocol. Self-collections by custodians may give rise to questions regarding the accuracy of collections if directions and oversight are poor or non-existent.

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

RESOURCES AND AUTHORITIES

Serra Chevrolet, Inc. v. General Motors Corp., 446 F.3d 1137, 1147 (11th Cir. 2006) (affirming portion of district court's ruling related to failure to comply with discovery order where defendant did not conduct a manual search of its files until several months after being ordered to produce all documents related to a particular subject).

12. Absent party agreement or court order specifying the form or forms of production, production should be made in the form or forms in which the information is ordinarily maintained or in a reasonably usable form, taking into account the need to produce reasonably accessible metadata that will enable the receiving party to have the same ability to access, search, and display the information as the producing party where appropriate or necessary in light of the nature of the information and the needs of the case.

Comment 12.a. Metadata

An electronic document or file usually includes not only the visible text but also hidden text, formatting codes, formulae, and other information associated with the file. These many types of ancillary information are often lumped together as "metadata," although some distinctions between different types of metadata should be recognized.

For example, the two most common distinctions are between "application" metadata and "system" metadata. Application metadata is created as a function of the application software used to create the document or file. Common application metadata instructs the computer how to display the document (for example, the proper fonts, spacing, size, and color). Other application metadata may reflect modifications to the document, such as prior edits or editorial comments. This metadata is embedded in the file it describes and moves with the file when it is moved or copied. System metadata reflects information 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. System metadata generally is not embedded within the file it describes, but is stored externally elsewhere on the organization's information management system. Depending on the circumstances of the case, the content value of a particular piece of metadata may be critical or may be completely irrelevant. It may be important, therefore, when planning the scope of discovery to determine the types and locations of metadata associated with the various application data types that will be targeted in the discovery and determine whether or not they may play an ongoing role.

Aside from its potential relation to the facts of the case, metadata may also play a functional role in the usability of electronically stored information. For example, system metadata may allow for the quick and efficient sorting of a multitude of files by virtue of the dates or other information captured in metadata. In addition, application metadata may be critical to allow the functioning of routines within the file, such as cell formulae in spreadsheets.

Care should be taken when using metadata, as the content of a given piece of metadata may convey information that is contextually inaccurate. For example, when a Microsoft Word™ document is created, the computer on which that document is saved may automatically assign the document an "author" based on the information available on that computer. That document may be used as a template by other persons, but the "author" information is never changed. Thus, subsequent iterations of the document may carry as an "author" a person with no knowledge of the content of the document. Accordingly, a proper and thorough analysis should be undertaken in order to properly assess how the metadata was created.

The extent to which metadata should be preserved and produced in a particular case will depend on the needs of the case. Parties and counsel should consider: (a) what metadata is ordinarily maintained; (b) the potential relevance of the metadata to the dispute (e.g., is the metadata needed to prove a claim or defense, such as the transmittal of an incriminating statement); and (c) the importance of reasonably accessible metadata to facilitating the parties' review, production, and use of the information. In assessing preservation, it should be noted that the failure to preserve and produce metadata may deprive the producing party of the opportunity later to contest the authenticity of the document if the metadata is material to that determination. Organizations should evaluate the potential benefits of retaining native files and metadata (whether or not it is produced) to ensure that documents are authentic and to preclude the fraudulent creation of evidence.[37]

RESOURCES AND AUTHORITIES

Shira A. Scheindlin and Jonathan M. Redgrave, *Discovery of Electronic Information, 2 Bus. & Commerical Litig. in Fed. Courts,* §22:22 (Robert L. Haig ed., 2005 & Supp. 2006).

Kentucky Speedway, LLC v. NASCAR, Inc., Civ. No. 05-138-WOB, 2006 W.S. Dist. Lexis 92028 (E.D. Ky. Dec. 18, 2006) (court declines to require defendant to supplement production of electronically stored information, relying on a perceived emerging presumption against the production of metadata and citing Sedona Principle 12 (2005 edition)).

In re Priceline.com Inc. Sec. Litig., 233 F.R.D. 88, 91 (D. Conn. 2005) ("Defendants shall produce responsive information contained in stored data files to plaintiffs in TIFF or PDF form with Bates numbering and appropriate confidentiality designations, shall produce searchable metadata databases, and shall maintain the original data itself in native format for the duration of the litigation.").

Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 643 (D. Kan. 2005) (*"Williams I"*)(finding that if production of spreadsheets are ordered to be produced in form in which they are maintained, metadata should be produced, citing *The Sedona Principles* for definition and discussion of metadata).

Comment 12.b. Formats used for collection and production: "ordinarily maintained" v. "reasonably usable"

Electronically stored information is fundamentally different from paper information in that it is dynamic, created and stored in myriad different forms, and contains a substantial amount of nonapparent data. Because of these differences, approaching the production of electronically stored information as though it is just the modern equivalent of a paper document collection will likely lead to a failure to fully consider the complex issues involved and a failure to select the most relevant and functional form of production for a particular type of electronic information.

[37] Several attorney disciplinary bodies have issued opinions on the dangers of counsel inadvertently transmitting attorney-client confidences as metadata embedded within electronic documents and the efficacy of receiving counsel searching for and viewing such metadata. *See, e.g.,* New York Ethics Op. 749 (2001); ABA Comm. on Ethics And Prof'l Responsibility, Formal Op. 06-442; New York Ethics Op. 749 (2001); Maryland Bar Assoc. Comm. on Ethics Op. 2007-09. The Working Group expresses no opinion on these decisions, and it should be noted that the issues discussed in these opinions usually arise in a transactional context, before any duty to preserve electronically stored information relevant to anticipated or pending litigation arises. In transactional settings, counsel is free to routinely employ so-called "metadata scrubbers" to remove unwanted metadata before transmitting electronic documents to clients or to other counsel. In deciding to do so, counsel should weigh the dangers of transmitting client confidences or attorney-client communication against the benefits that metadata provides for later document management, indexing and review, and may choose to "scrub" only certain categories of particularly sensitive metadata. Once litigation is anticipated, however, routine metadata scrubbing of relevant documents must be reexamined in light of the preservation duty.

Electronic information is created and stored by a computer in a file format "native" to the software application used to create or utilize the information. However, electronically stored information can be produced in any number of formats, some more useful than others. For example, although an email message may be readily understood when presented as plain text printed on paper, this is not the case with audio or video files. All electronic documents and files, to one extent or another, contain information that is not apparent when displayed on a screen, printed on paper, or heard on speakers. The extent to which a production of electronically stored information includes such data depends on the form of production. For example, electronic information produced in the form in which the file was created (or "native format") will contain application metadata such as formulae in spreadsheets or "tracked changes" in word processing documents.

An electronic document or file produced in native format may also be accompanied by system metadata, such as the date the file was created or the identity of the computer on which it was created. However, electronic information produced in a static, two-dimensional form, such as an image file (e.g., TIFF or PDF, explained below), while having some practical advantages, does not contain any of the original metadata. Certain types of electronic information, such as databases, simply cannot be converted from their native, dynamic, three-dimensional form without significant loss of information and functionality.

Accordingly, there should be two primary considerations in choosing the form of production: (1) the need for, or probative value of both apparent and metadata; and (2) the extent to which the production of metadata will enhance the functional utility of the electronic information produced and allow the parties to conduct a more cost-effective and efficient review. These considerations should be weighed against the negative aspects associated with each format.[38] For example, production in a "native" format entails both advantages and disadvantages. Native production, which generally includes the entire file and associated metadata, may afford the requesting party access to the same information and functionality available to the producing party and, from a technical perspective, usually requires minimal processing before production. However, information produced natively may be difficult or impossible to redact or Bates number, and files in their native forms must be viewed using applications capable of opening and presenting the information without alteration. Suitable applications are not always accessible to requesting parties, who may also lack the equipment or expertise required to use such applications.

A native file production that includes a substantial volume and variety of file types could become very expensive and burdensome for the requesting party. In addition, since certain metadata could contain or reveal privileged, secret, or other sensitive information, an organization may determine that it must review such metadata before producing it, which can substantially impact the speed of production.

In current practice, many parties, local rules and courts have endorsed the use of image production formats, principally the Tagged Image File Format ("TIFF") and Adobe Portable Document Format ("PDF") formats. Standing by themselves, image file productions are the equivalent of printed pages from the screen. They have the advantage of a static format that can be Bates numbered and redacted, and, compared to native files, it is harder (but not impossible) to alter the data inadvertently or deliberately. However, simple image productions require significant processing that is time consuming and costly. The image productions, by themselves, also lose searchable text and metadata that might enable better understanding and utility of the evidence.

In an effort to replicate the usefulness of native files while retaining the advantages of static productions, image format productions are typically accompanied by "load files," which are ancillary files that may contain textual content and relevant system metadata. Again, however, there are potentially significant costs inherent in this process, and it does not work well for certain types of electronically stored information such as spreadsheets and dynamic databases.

---

[38] *See The Sedona Canada Principles*, Principle 8, Comment 8.b (2006), *available at* http://www.thesedonaconference.org.

The routine preservation of metadata pending agreements or decisions on the ultimate form of production may be beneficial in a number of ways. Preservation of metadata may provide better protection against inadvertent or deliberate modification of evidence by others and the systematic removal or deletion of certain metadata may involve significant additional costs that are not justified by any tangible benefit. Moreover, the failure to preserve and produce metadata may deprive the producing party of the opportunity later to contest the authenticity of the document if the metadata would be material to that determination.

In amending Rule 34(b) to accommodate the production of electronically stored information, the Advisory Committee acknowledged that wherever possible, parties should first attempt to reach agreement on the various form or forms of production, given that different types of data may serve different purposes and the need for native production and metadata may vary. The Advisory Committee also recognized that the default forms of production appropriate to paper discovery did not have direct equivalents in electronic discovery. However, the goals furthered by providing default forms of production governing paper discovery should be the same in electronic discovery – to encourage forms of production that would be inexpensive for the producing party and reasonably useable for the requesting party; and to avoid costly data conversion on the one hand, and the electronic equivalent of the "document dump" on the other hand. Therefore, without mandating any particular form of production, Rule 34(b) provides that in the absence of agreement or a specific court order, a producing party should produce electronically stored information either in the form in which it is "ordinarily maintained" or in a "reasonably usable" form.

The form in which electronically stored information is "ordinarily maintained" is not necessarily synonymous with the form in which it was created. There are occasions when business considerations involve the migration or transfer of electronically stored information to other applications or systems. For example, customer information may routinely be gathered by an organization from Internet-based forms, then collected in a relational database for further business use. The information may be incorporated into Microsoft Word™ documents, such as memoranda or correspondence, which may later be transferred into static electronic images for long-term storage and retrieval. In such cases, the form in which the electronically stored information is maintained understandably varies from that in which it was obtained or created. Absent an attempt to deliberately downgrade capabilities or characteristics for the purposes of avoiding obligations during specific litigation, migration to alternative forms for business purposes is not considered inconsistent with preservation obligations.

What constitutes a "reasonably usable" form will depend on the circumstances of a case, given that the need for email, documents, spreadsheets, or dynamic databases can all vary. As noted earlier, selection of a "reasonably usable" form is best handled by an agreement between the parties regarding the distinct categories of electronically stored information sought in a case. But where such an agreement is not reached, the Committee Note to Rule 34(b) explicitly states that "[i]f the responding party ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, the information should not be produced in a form that removes or significantly degrades this feature." Accordingly, a party should produce electronically stored information in "reasonably usable" forms, though not necessarily "native format."

In determining the appropriate forms of production in a case, requesting parties and counsel should consider: (a) the forms most likely to provide the information needed to establish the relevant facts of the case; (b) the need for metadata to organize and search the information produced; (c) whether the information sought is reasonably accessible in the forms requested; and (d) the requesting party's own ability to effectively manage and use the information in the forms requested.

Producing parties and counsel should consider: (a) the relative risks of inadvertent production of confidential, privileged, and work product information associated with different forms of production; (b) difficulties in redaction, tracking, and use of native files; (c) whether alternative (e.g., "nonnative") forms of production provide sufficient usability (e.g., by providing adequate accompanying information through load files) such that the producing and requesting parties have the same access to functionality; and (d) the relative costs and burdens with respect to the proposed forms of production, including the costs of preproduction review, processing, and production.

Illustration i. A party demands that responsive documents, "whether in hard copy or electronic format," be produced. The producing party objects to producing the documents in native electronic format and states that production will be made through PDF or TIFF images on CD-ROMs with load files containing electronically searchable text and selected system and application metadata. The requesting party raises no further objection, and the producing party produces photocopies of the relevant hard copy memoranda, emails and electronic records in a PDF or TIFF format accompanied by a load file containing the searchable text and selected metadata for each item of electronically stored information. This production of electronically stored information satisfies the goals of Principle 12 because the production is in usable form, e.g., electronically searchable and paired with essential metadata.

Illustration ii. Plaintiff claims that he is entitled to a commission on a transaction, based upon an email allegedly sent by the president of defendant corporation agreeing to the commission. Defendant asserts that there is no record of the email being sent in its email system or the logs of its Internet activity, and that the email is not authentic. In these circumstances, it is appropriate to require production of not only the content of the questioned email but also of the email header information and metadata, which can play a crucial role in determining whether the questioned message is authentic.

Illustration iii. Plaintiff alleges that the defendant engaged in a fraud regarding software development. The plaintiff seeks a preliminary order permitting direct access to the hard drives of the software engineers involved and demonstrates that the computer program sold by defendant appears to incorporate plaintiff's source code. In this case, production of the source code in native format may be appropriate, as well as targeted forensic examination of the hard drives concerning the development of the source code. The court should impose such conditions as it deems appropriate to protect legitimate property and privacy interests of the defendant and its employees.

RESOURCES AND AUTHORITIES

Kentucky Speedway, LLC v. NASCAR, Inc., Civ. No. 05-138-WOB, 2006 U.S. Dist. Lexis 92028 (E.D. Ky. Dec. 18, 2006) (court declines to require defendant to supplement production of electronically stored information, relying on a perceived emerging presumption against the production of metadata and citing Sedona Principle 12 (2005 edition)).

In re Priceline.com Inc. Sec. Litig., 233 F.R.D. 88, 91 (D. Conn. 2005) ("Defendants shall produce responsive information contained in stored data files to plaintiffs in TIFF or PDF form with Bates numbering and appropriate confidentiality designations, shall produce searchable metadata databases, and shall maintain the original data itself in native format for the duration of the litigation.").

Compare Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 652 (*"Williams I"*) (D. Kan 2005) ("[W]hen a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to the production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order."), *with Williams v. Sprint/United Mgmt. Co.,* 2006 WL 3691604 (D. Kan. December 12, 2006) (*"Williams II"*) "Defendant raises legitimate concerns about producing the transmittal e-mails with their attachments in their native format, including the whether production in native format would permit the redaction or removal of privileged information. […] Moreover, even assuming that Defendant could produce the transmittal e-mails together with their attachments in native format with the privileged information redacted, Plaintiffs have not sufficiently explained why they need the transmittal e-mails in their native format.").

Comment 12.c. Procedure for requesting and producing metadata under the Federal Rules

Amended Rule 26(f), concerning the conference of parties and planning for discovery, broadly requires parties to address issues related to electronically stored information early in cases where such discovery is at issue. Specifically, Rule 26(f)(3) mandates that the parties meet, confer, and develop a proposed discovery plan that indicates the parties' views and proposals regarding, among other topics, "any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced." To the extent that the parties believe that production of metadata is needed because of either relevance or usability, that should be raised at this conference as it will be a consideration in determining both the need to preserve information in a particular form and the ultimate form or forms of production. By fostering early and ongoing communication between the parties on the issue, the amendments to Rules 26(f) and 34 are designed to lessen the likelihood that disputes over form of production (including metadata issues) will impact the orderly progression of discovery.

Absent an agreement or a court order, Rule 34 establishes a distinct procedure for electronically stored information. Under Rule 34(b), a party serving a request for the production of electronically stored information may, but is not required to, specify the form or forms in which the information should be produced. To the extent that the requesting party seeks a "native" production or some other form of production with accompanying metadata, the revised rule places a burden on the party to make that request explicit. If the requesting party specifies a form or forms of production, the responding party may object to the requested form or forms of production and state the reasons for the objection. Regardless of whether a requesting party fails to state a preferred form of production, or the responding party objects to a requested form, the responding party must state the form or forms in which it intends to produce electronically stored information. In both cases, the producing party should indicate with specificity the forms of production it proposes to use and the requesting party should scrutinize the proposed forms.

Absent party agreement or court order providing otherwise, the responding party must produce electronically stored information in one of two "default forms," the form "in which it is ordinarily maintained," or a form that is "reasonably usable." *See* Comment 12b, *supra*. In addition, absent an agreement or order, a party need not produce the same electronically stored information in more than one form.

Any disputes regarding form or forms of production may be brought before a court for resolution in a variety of ways. The parties may raise any inability to reach agreement at the Rule 16(b) conference so that the court can give initial guidance. The court may place the issue on the calendar for formal resolution, recognizing the possible need for evidence from experts, IT personnel and business users. Parties may also raise the issue by motions – either a motion to compel by the requesting party under Rule 37 or a motion for a protective order by the responding party under Rule 26(c). However, the rules require, and the courts encourage, the parties to attempt to meet and resolve any dispute before filing such motions.

Finally, it is worth noting that a growing tendency in some federal courts is to issue formal local rules or informal guidelines, standards, or "default" case management recommendations addressing electronic production formats. There is much to be gained by such experimentation, but a serious risk exists that these will lead to rigidity and defeat the purpose of the Amended Rules to require parties, not courts, to make the tough choices that fit the particular discovery needs of a case.

RESOURCES AND AUTHORITIES

D. Kan., *Guidelines for Disc. of Electronically Stored Information, available at* http://www.ksd.uscourts.gov/guidelines/electronicdiscoveryguidelines.pdf.

D. Md. Loc. R., *Suggested Protocol for Disc. of Electronically Stored Information, available at* http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf.

N.D. Ohio Civ. App. K, *Default Standard for Discovery of Electronically Stored Information ("E-Discovery"), available at* http://www.ohnd.uscourts.gov/Clerk_s_Office/Local_Rules/AppendixK.pdf.

Comment 12.d. Parties need not produce the same electronically stored information in more than one format

Provided that the forms of production are reasonable, a party should not be required to produce the same information in both hard copy and electronic format, or in both native format and another electronic format. The 2006 Amendments state that production in more than one format is not required, absent an agreement or order. *See* Fed. R. Civ. P. 34(b)(2)(iii). If a court requires production of the same information a second time in a different format because of an unclear or tardy request, the court should consider shifting some or all of the cost of the second production to the requesting party.

RESOURCES AND AUTHORITIES

Williams v. Owens Illinois, Inc., 665 F.2d 918, 933 (9th Cir. 1982) (appellants in employment discrimination case not entitled to computer tapes when they already had access to wage cards containing the same information, even though using the cards "may be more time-consuming, difficult, and expensive").

In re Bristol-Meyers Squibb Sec. Litig., 205 F.R.D. 437, 443 (D.N.J. 2002) (plaintiff not required to pay half of defendant's scanning costs for electronic documents, even though defendant had already produced documents in paper form; although plaintiff was entitled to electronic version, it was already obligated to pay half of photocopying costs for the paper documents and should not be forced to pay for "double-discovery").

Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 652 (D. Kan 2005) (*"Williams I"*) ("When a party is ordered to produce electronic document spreadsheets as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to the production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order.").

13. Absent a specific objection, party agreement or court order, the reasonable costs of retrieving and reviewing electronically stored 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 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 may be shared by or shifted to the requesting party.

Comment 13.a. Factors for cost-shifting

The ordinary and predictable costs of discovery are fairly borne by the producing party. However, Rule 26 has long empowered courts to shift costs where the demand is unduly burdensome because of the nature of the effort involved to comply.

Traditionally, the consideration of cost-shifting by the courts has been at the discretion of the court.[39] Amended Rule 26(b)(2)(B) specifically notes that an order compelling the production of electronically stored information that is "not reasonably accessible"[40] may be subject to conditions, including "payment by the requesting party of part or all of the reasonable costs of obtaining information from sources that are not reasonably accessible." The Rule then identifies seven factors to be considered, and it is likely that courts addressing production under this rule will routinely consider, if not order, cost-shifting or cost sharing. The types of information that typically may (but not always) fall within Rule 26(b)(2)(B) include deleted data, disaster recovery/backup tapes, residual data, and legacy data.

Importantly, parties should recognize that cost-sharing and cost-shifting remains separately available under Rule 26(b)(2)(C) and Rule 26(c). In particular, even though electronically stored information is reasonably accessible (e.g., it exists on a corporate storage area network), the aggregate volume of data requested may be disproportionate to the needs in the case and/or the respective resources of the parties (e.g., a large multinational company suing a small company) such that a condition of further discovery can be the shifting of some or all costs of such discovery.

The factors for cost-shifting for the production of burdensome electronically stored information (whether reasonably available or accessible or not) should include (in order of importance):

1. whether the information is reasonably accessible as a technical matter without undue burden or cost
2. the extent to which the request is specifically tailored to discover relevant information
3. the availability of such information from other sources, including testimony, requests for admission, interrogatories, and other discovery responses
4. the total cost of production, compared to the amount in controversy
5. the total cost of production, compared to the resources available to each party
6. the relative ability of each party to control costs and its incentive to do so
7. the importance of the issues at stake in the litigation, and
8. the relative benefits to the parties of obtaining the information.

Finally, consideration of the "total cost of production" includes the estimated costs of reviewing retrieved documents for privilege, confidentiality, and privacy purposes. It also includes consideration of opportunity costs or disruption to the organization, *e.g.,* the need to redirect IT staff from business projects to retrieve or review the data. Accordingly, Rule 26 broadly defines the burdens that can be considered by a court in the proportionality analysis.

---

[39] Notably, the Advisory Committee Note also provides that "a requesting party's willingness to share or bear the access costs may be weighed by the court in determining whether there is good cause."

[40] Principle 13 uses the term "available" whereas the Federal Rule uses "accessible." In practice, there should be no practical difference as the focus should be on how the information is generally stored and used (i.e., in the regular course of business or not) and how hard (i.e., burdensome and expensive) it is to retrieve and review it.

RESOURCES AND AUTHORITIES

Conference of Chief Justices, *Guidelines For State Trial Courts Regarding Discovery of Electronically Stored Information,* Guideline 7 (Aug. 2006) ("Reallocation of Discovery Costs") (listing seven factors for courts to use in determining whether to shift part or all of the costs of discovery costs of information which is not accessible).

Comment, *The Growth of Cost-Shifting in Response to the Rising Cost and Importance of Computerized Data in Litigation,* 59 Okla. L. Rev. 115 (2006).

ABA Civil Discovery Standards, (1999) (rev. Aug. 2004) Standard 29(b)(iv) *available at* http://www.abanet.org/litigation/discoverystandards/2004civildiscoverystandards.pdf (listing factors to consider in allocating costs of discovery of any form of electronic information or related software).

Corrine L. Giacobbe, *Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronically Stored Data,* 57 Wash. & Lee L. Rev. 257 (2000).

Martin H. Redish, *Electronic Discovery and the Litigation Matrix,* 51 Duke L.J. 561 (2001).

Tex. R. Civ. P. 196.4 (mandating that requesting party "pay reasonable expenses of any extraordinary steps required to retrieve and produce" any information requested which is not "reasonably available").

Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 431 (S.D.N.Y. 2002) (shifting costs of production of email from backup tapes in order to protect parties from undue burdens and costs under Rule 26(c) after a balancing approach involving specificity, likelihood of recovery of critical information, availability of information from other sources, purposes for which maintained, relative benefit, total costs associated with production, relative ability to control costs and resources), *affirmed*, No. 98 Civ. 8272(RPP), 2002 WL 975713 (Patterson, J.) (S.D.N.Y. May 9, 2002).

Wiginton v. CB Richard Ellis, Inc., No. 02-C-6832, 229 F.R.D. 568, 573 (N.D. Ill. Aug. 9, 2004) (holding that the "importance of the requested discovery in resolving the issues of the litigation" should be considered for cost-shifting in addition to the factors in the *McPeek, Rowe,* and *Zubulake* cases, and finding that these factors required defendant to bear 25 percent and plaintiffs 75 percent of the costs of restoring defendant's backup tapes, searching them and transferring them to an electronic viewer).

Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 318-22 (S.D.N.Y. 2003) (*"Zubulake I"*) (noting that "whether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format," and formulating seven-factor test for determining whether cost-shifting might be appropriate).

Zubulake v. UBS Warburg LLC, 216 F.R.D. 280, 290 (S.D.N.Y. 2003) (*"Zubulake III"*) (applying seven-factor test and shifting one-fourth of costs associated with restoring and searching backup tapes, but excluding cost of production, such as costs incurred when reviewing documents for privilege, from consideration in determining that total cost of production).

Comment 13.b. Cost-shifting cannot replace reasonable limits on the scope of discovery

Shifting the costs of extraordinary electronically stored information discovery efforts 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. The courts should discourage burdensome requests that have no reasonable prospect, given the size of the case, of significantly contributing to the discovery effort, even if the requesting party is willing to pay.

> *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. 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 at least a portion of the costs associated with the request.

Comment 13.c. Non-party requests must be narrowly focused to avoid mandatory cost-shifting

Since 1991, Rule 45 of the Federal Rules has required persons issuing subpoenas to take reasonable steps to avoid imposing undue burdens or expense on the requested party and, if objection is made, any order to compel production "shall protect [the requested party] from significant expense." As important, the Committee Notes to the 1991 amendments state:

> A non-party required to produce documents or materials is protected against significant expense resulting from involuntary assistance to the court .... The court is not required to fix the costs in advance of production, although this will often be the most satisfactory accommodation to protect the party seeking discovery from excessive costs. In some instances, it may be preferable to leave uncertain costs to be determined after the materials have been produced, provided that the risk of uncertainty is fully disclosed to the discovering party.

In support of this proposition, the Committee cited a 1982 decision from the Ninth Circuit in a case where non-parties produced more than six million documents, and the costs of non-party discovery exceeded two million dollars. In light of the potentially enormous burdens involved with non-party discovery involving electronically stored information, parties seeking information from non-parties have a substantial interest in narrowly tailoring requests in light of a greater likelihood that a court may impose cost-sharing or cost-shifting. Indeed, parties seeking information from non-parties should be prepared to address these issues at informal meetings to determine if disputes can be resolved by agreement instead of rulings on a motion to quash or a motion to compel.

RESOURCES AND AUTHORITIES

United States v. Columbia Broadcasting Sys., Inc., 666 F.2d 364, 371 (9th Cir. 1982) ("[n]on-party witnesses are powerless to control the scope of litigation and discovery and should not be forced to subsidize an unreasonable share of the costs of a litigation to which they are not a party.").

14. Sanctions, including spoliation findings, should be considered by the court only if it finds that there was a clear duty to preserve, a culpable failure to preserve and produce relevant electronically stored information, and a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.

Comment 14.a. Intentional, reckless, or grossly negligent violations of preservation obligations

Due to the complexity of modern electronic information systems, the large volumes of electronically stored information, and the continuing changes in information technology, there exists a potential for good faith errors or omissions in the process of identifying, preserving and producing relevant electronically stored information, which involves both humans and technology. This reality is based in part on recognition that routine business operations necessarily include functions that continuously modify, overwrite and delete data.

Case law indicates that there must be a sufficient level of culpability to support the imposition of spoliation sanctions. Accordingly, neither spoliation findings nor sanctions should issue without proof of a knowing violation of an established duty to preserve or produce electronically stored information or a reckless disregard amounting to gross negligence. Usually, the knowing violation will be found in the context of a specific provision of an existing discovery order, subpoena, preservation order, or similar explicit preservation obligation. However, the common law duty of preservation arises when a party, either plaintiff or defendant, reasonably anticipates litigation.[41]

The nature, scope and execution of preservation obligations are covered generally in Principle 5. Other related Principles are Principle 2 (role of proportionality standard), Principle 3 (necessity for early consultation), Principle 6 (proper role of producing parties in selecting methods of preservation), Principle 7 (burden of proof in proving inadequate preservation), Principle 9 (limits on duty to preserve deleted information), Principle 11 (use of sampling in regard to preservation) and Principle 12 (preservation of metadata).

RESOURCES AND AUTHORITIES

Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108 (2d Cir. 2002) (stating that sanctions may be appropriate for negligent failure to take adequate steps to preserve and produce ESI in a timely manner).

Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 746-47 (8th Cir. 2004) (adverse inference instruction should not be given on the basis of negligence alone; there must be a finding of bad faith or some other culpable conduct, such as the ongoing destruction of documents during litigation and discovery even after they have been specifically requested).

Morris v. Union Pac. R.R. Co., 373 F.3d 896, 900-01 (8th Cir. 2004) (warning that an adverse inference instruction is a powerful tool which, when not warranted, creates a substantial danger of unfair prejudice, ruling that there must be a finding of intentional destruction indicating a desire to suppress the truth, and, in light of the trial court's conclusion that defendant did not intentionally destroy an audiotape of a collision, reversing and remanding for a new trial).

---

[41] *Compare Hynix Semiconductor, Inc. v. Rambus, Inc.*, No. C-00-20905 RMW (N.D. Cal. January 4, 2006) ("reasonable anticipation of litigation" when party is defendant) *with Rambus, Inc. v. Infineon Technologies AG,* 220 F.R.D. 264 (E.D. Va. 2004) ("reasonable anticipation of litigation" when same party, under same circumstances, is plaintiff).

Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc., No. 502003CA005045XXOCAI, 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005) (after concluding that defendant had sought to thwart discovery and failed, through willful and gross abuse, grossly negligent and negligent conduct with respect to discovery obligations to timely locate and produce relevant information from more than 1,000 backup tapes, court determines that (i) *defendant* would bear the burden of proving to the jury by the greater weight of the evidence that it lacked knowledge of fraud and did not aid, abet or conspire to perpetrate fraud and (ii) court would read to the jury a statement of "conclusive" findings of fact concerning the discovery failures from which the parties could argue in favor of whatever inferences the facts may support); *further opinion* 2005 WL 674885 (Fla. Cir. Ct. Mar. 23, 2005) (determined that partial default should be entered, following which jury returned verdicts of $605 million in compensatory damages and $850 million in punitive damages), r*ev'd and remanded on other grounds,* ---So.2d ---, 2007 WL 837221 (Fla. Dist. Ct. App. Mar. 21, 2007).

Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 431-33 (S.D.N.Y. 2004) (*"Zubulake V"*) (for willful destruction where certain key employees destroyed email after being repeatedly told by counsel not to, and counsel failed to interview key players in litigation or do key word search of databases in course of creating and enforcing litigation hold).

Comment 14.b. "Negligent" versus "culpable" spoliation

Some courts have invoked the tort concept of negligence in addressing spoliation of evidence claims. It is critical, however, to understand that establishing a standard of care (e.g., negligence) does not answer the question of whether any sanction is warranted. In considering sanctions, the focus should be on culpability and prejudice. As to culpability, the question is whether in the circumstances of the case, a party is sufficiently culpable for the loss of electronic data. "Culpability" in most jurisdictions does not include what could be considered "negligent conduct." Even courts that state that culpability may include negligent destruction – or, more precisely, negligent failure to preserve -- do equate such conduct with an entitlement to sanctions for data loss. Regardless of the label applied, courts begin by examining whether the party took reasonable good faith efforts to preserve relevant electronic data. The more evidence that the failure was intended to prevent discovery of specific information, the more likely spoliation instructions or other sanctions will be imposed. If a party has specifically requested documents in electronic format, allowing those documents to be destroyed, even if hard copies of those documents still exist, can lead to sanctions.

On the other hand, if a court finds that relevant information has been negligently lost, resulting in prejudice to the requesting party, but without the level of culpability that would lead to sanctions, the court may nevertheless order remedial measures designed to put the parties in roughly the position they would have been but for the negligence of the responding party. Such remedial measures may include ordering further discovery or allocating costs.

RESOURCES AND AUTHORITIES

Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 108 (2d Cir. 2002) (stating that sanctions may be appropriate for negligent failure to take adequate steps to preserve and produce electronically stored information in a timely manner).

Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 746-47 (8th Cir. 2004) (adverse inference instruction should not be given on the basis of negligence alone; there must be a finding of bad faith or some other culpable conduct, such as the ongoing destruction of documents during litigation and discovery even after they have been specifically requested).

Morris v. Union Pac. R.R., 373 F.3d 896, 900-01 (8th Cir. 2004) (warning that an adverse inference instruction is a powerful tool which, when not warranted, creates a substantial danger of unfair prejudice, ruling that there must be a finding of intentional destruction indicating a desire to suppress the truth, and, in light of the trial court's conclusion that defendant did not intentionally destroy an audiotape of a collision, reversing and remanding for a new trial).

Comment 14.c. Prejudice

A party seeking sanctions must prove that there is a reasonable likelihood that it has been materially prejudiced by the alleged spoliation. Destruction of tangentially relevant information, or information that is duplicative and has been produced from other sources, does not constitute prejudice.

An award of sanctions without a showing of prejudice is particularly inappropriate in the context of the discovery of electronically stored information, which often involves large volumes of complex data, in which it can be difficult to identify, preserve, and produce all relevant information with complete accuracy. In addition, in light of the significant confusion and disagreement about the proper treatment of metadata in cases and relevant literature – from preservation through production – it would be inappropriate to award sanctions simply due to the loss of metadata without a demonstration of actual prejudice.

The timeliness of a challenge to production failures may indicate prejudice, or the lack of it. The amended Federal Rules of Civil Procedure, as well as *The Sedona Principles,* since their inception, have urged an early constructive dialogue in cases between parties regarding respective preservation obligations and expectations. A corollary to this early discussion is that untimely challenges to production failures should not provide a basis for the imposition of sanctions.

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

RESOURCES AND AUTHORITIES

Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 221 (S.D.N.Y. Oct. 22, 2003) (*"Zubulake IV"*)("In order to receive an adverse inference instruction, Zubulake must demonstrate not only that UBS destroyed relevant evidence as that term is ordinarily understood, but also that the destroyed evidence would have been favorable to her.").

Comment 14.d. Good faith

Many cases involving spoliation and sanctions examine the "good faith" of the party that lost the evidence. Rule 37(f) now incorporates this standard, stating that a sanction should not issue if electronically stored information is lost as a result of the "routine, good-faith" operation of an electronic information system.

Good faith has both subjective and objective aspects in the context of electronic discovery. Considerations of a party's "good faith" may include the following inquiries: (a) was there a standard litigation hold process and was it followed? (b) did the party adequately communicate litigation hold instructions to employees? (c) did the party periodically distribute litigation hold reminders? (d) did the party adequately investigate and identify the locations that were reasonably likely to contain unique and relevant electronically stored information? (e) has the party been cooperative and forthcoming in Rule 26(f) and Rule 16(b) discussions? (f) has the party been reasonable and forthcoming in written discovery responses and depositions? (g) did the party take steps to secure relevant, unique electronically stored information that would otherwise be overwritten or deleted by automatic processes? (h) did the party take reasonable steps to ascertain whether orphaned or legacy data contain relevant information? and (i) was the electronic system designed and implemented solely with the intent of meeting business and technical needs or with the intent of thwarting discovery?[42] There is no talismanic test of "good faith," but organizations that can answer most if not all of these questions in the affirmative should be presumed to have acted in good faith absent proof to the contrary.

[42] *See* Fed. R. Civ. P. 37 Committee Note ("Many steps essential to computer operation may alter or destroy information, for reasons that have nothing to do with how that information might relate to litigation. […] Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation."). Fed. R. Civ. P. 37(f) is anticipated to be renumbered Fed. R. Civ. P. 37(e) effective December 1, 2007. *See* footnote 3, *supra*.

RESOURCES AND AUTHORITIES

Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 745-49 (8th Cir. 2004) (adverse inference instruction for pre-litigation destruction of evidence through a document retention program cannot be based on negligence alone but requires a finding of bad faith).

Lewy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988) (in reviewing whether documents destroyed pursuant to an existing retention policy constituted sanctionable conduct, court should determine whether the length of retention is reasonable given the particular type of document, whether lawsuits that would require production of these documents have been filed and their frequency, and whether the document retention policy was instituted in bad faith).

Comment 14.e. The good-faith destruction of electronically stored documents and information in compliance with a reasonable records management policy should not be considered sanctionable conduct absent an organization's duty to preserve the documents and information.

Where a party destroys documents or electronically stored information in good faith under a reasonable records management policy, no sanctions should attach. This does not mean a party may use its records management policy as a pretext for destroying documents or electronically stored information with impunity. Once a party reasonably determines that electronically stored information in its custody or control may be relevant to pending or reasonably foreseeable litigation, the party should take reasonable steps to preserve that electronically stored information, even if its records management program calls for its routine destruction. Determining a party's duty to preserve requires answering two separate questions: "when does the duty to preserve attach?" and "what evidence must be preserved?" Failure to properly preserve information may result in sanctions, including monetary fines, instructions to the jury commanding them to infer that the destroyed documents would be adverse to the interests of the responding party, and, in extreme cases, default judgments. Therefore, an organization's records management policy should recognize that the organization will sometimes have to suspend its ordinary retention and disposition of records and should include procedures designed to implement such suspensions.

However, if a party does not reasonably anticipate litigation, the destruction of documents in compliance with a reasonable records management policy should not be considered sanctionable conduct. Instead, the fact that the destruction occurred in compliance with a preexisting policy should be considered *prima facie* evidence of the good faith of the organization. In the absence of a duty to preserve records, courts have consistently refused to sanction parties who have destroyed records pursuant to a records retention program. Likewise, if duplicative or redundant information is routinely destroyed, but all relevant information has been preserved, courts have consistently refused to sanction parties in the absence of prejudice to the requesting party.

RESOURCES AND AUTHORITIES

Arthur Andersen LLP v. U.S., 544 U.S. 696, 704 (2005) ("'Document retention policies,' which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business …. It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.").

Morris v. Union Pac. R.R., 373 F.3d 896, 902 (8th Cir. 2004) (failure to interrupt recycling of audiotape despite occurrence of potentially discoverable information is not sanctionable in light of lack of intentional destruction indicating a desire to suppress the truth).

Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 747 (8th Cir. 2004) (holding that "some indication of an intent to destroy the evidence for the purpose of obstructing or suppressing the truth" is required to issue an adverse inference sanction where information is destroyed through the routine operation of a document retention policy).

Appendix A
Table of Authorities

Federal Cases

State Cases

Federal Statutes and Regulations

Federal Court Rules

State Court Rules

Ethics and Professional Responsibility Citations

Books, Articles, and Commentaries

Appendix B

Suggested Cititation Format

This publication may be cited as follows:

> *The Sedona Principles, Second Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production (The Sedona Conference® Working Group Series, 2007).*

The recommended short citation form is simply:

> *The Sedona Principles, Second Edition (2007).*

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

> *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, Second Edition 3-4 (The Sedona Conference® Working Group Series, 2007).*

> *The Sedona Principles, Second Edition (2007), Principle 11.*

> *The Sedona Principles, Second Edition (2007), Cmt. 5.e.*

Appendix C

Working Group Members & Observers (as of May 3, 2007)

Woods Abbott
Raytheon Company

E. Regan Adams
Credit Suisse

Whitney Adams
Cricket Technologies

Sharon A. Alexander
Jones Day

Thomas Y. Allman
Mayer Brown Rowe & Maw LLP

Keith Altman
Finkelstein & Partners LLP

Andreas Antoniou
Paul, Weiss, Rifkind, Wharton & Garrison LLP

James R. Arnold
KPMG

Hon. Leonard B. Austin
Supreme Court of the State of New York
Observer

John Bacevicius
Gartner, Inc.

Denise E. Backhouse
Morgan Lewis & Bockius LLP

Wanda Bailey
McGuireWoods LLP

Jennifer V. Baker
Navigant Consulting Inc.

Craig Ball
Craig D Ball PC

Katherine L. Ball, M.D.
Johns Hopkins University, Division of Health Sciences Informatics

Laura Bandrowsky
Duane Morris LLP

John A. Bannon
Schiff Hardin LLP

Theodore S. Barassi
Symantec Corp.

Thomas I. Barnett
Sullivan & Cromwell

Jason R. Baron
National Archives and Records Admin.
Observer

Diane Barrasso
Barrasso Consulting LLC

Andre Barry
Cline, Williams, Wright, Johnson & Oldfather, LLP

Courtney Ingraffia Barton
LexisNexis Applied Discovery

Bobbi Basile
Ernst & Young LLP

Cynthia Bateman
Georgia Pacific Corporation

James A. Batson
Liddle & Robinson, LLP

John F. Baughman
Paul, Weiss, Rifkind, Wharton & Garrison LLP

Kirby D. Behre
Paul, Hastings, Janofsky & Walker, LLP

Lawrence P. Bemis
Kirkland & Ellis LLP

Adam S. Bendell
Strategic Discovery Inc.

Steven C. Bennett
Jones Day

Kara Benson
Faegre & Benson LLP

Hon. Richard E. Best, Ret.
Action Dispute Resolution Services
Observer

R. Eric Bilik
McGuireWoods LLP

Joanna Blackburn
Starbucks Coffee Company

Stephanie Blair
Morgan Lewis & Bockius LLP

Alan Blakley
RLS Legal Solutions

Marjorie Rosenthal Bloom
U.S. Pension Benefit Guaranty Corporation
Observer

Christopher Boehning
Paul, Weiss, Rifkind, Wharton & Garrison LLP

Hildy Bowbeer
3M

John J. Bowers
Womble Carlyle Sandridge & Rice PLLC

Kevin F. Brady
Connolly Bove Lodge & Hutz LLP

Richard G. Braman
The Sedona Conference
Ex Officio

Allison Brecher
Marsh & McLennan Co.

Appendix C

Working Group Members & Observers cont.

Kerry A. Brennan
Pillsbury Winthrop Shaw Pittman LLP

Julia Brickell
Altria Corporate Services, Inc.

Kelli J. Brooks
KPMG

Charlene Brownlee
Davis Wright Tremaine LLP

Greg Buckles
Attenex Corporation

Macyl Burke
ACT Litigation Services

Chistine M. Burns
Cohasset Associates, Inc.

Paul E. Burns
Gallagher & Kennedy, P.A.

William P. Butterfield
Cohen, Milstein, Hausfeld & Toll, PLLC

Kara Buzga
Milberg Weiss Barshad & Schulman LLP

Jonathan S. Campbell
Capital One Services, Inc.

Mary Beth Cantrell
Amgen Inc.

Jacquelyn A. Caridad
Morgan Lewis & Bockius LLP

Diane Carlisle
Baker Robbins & Company

Scott A. Carlson
Seyfarth Shaw LLP

Hon. John L. Carroll, Ret.
Cumberland School of Law at Samford University
Observer

Vincent Catanzaro
DuPont

Barbara Caulfield
Affymetrix, Inc.

M. Kate Chaffee
Faegre & Benson LLP

Lloyd B. Chinn
Proskauer Rose LLP

Thomas A. Clare
Kirkland & Ellis LLP

Michael A. Clark
EDDix LLC

Matthew Clarke
Ryley Carlock & Applewhite

R. Noel Clinard
Hunton & Williams LLP

Matthew Cohen
Alix Partners

Andrew M. Cohen
EMC Corporation

Adam Cohen
FTI

Sigmund J. Collins
Philip Morris U.S.A

Clark R. Cordner
Wilmer Cutler Pickering Hale and Dorr LLP

Alfred W. Cortese Jr.
Cortese PLLC

Christopher V. Cotton
Shook Hardy & Bacon LLP

Jim Coulson
Huron Consulting Group LLC

David Couzins
Wilmer Cutler Pickering Hale and Dorr LLP

Moze Cowper
Amgen Inc.

William Craco
Johnson & Johnson

Joyce Craig-Rient
Finnegan Henderson Farabow Garrett & Dunner LLP

Tim Crouthamel
State Farm Insurance Company

Conor R. Crowley
DOAR Litigation Consulting

Wendy Butler Curtis
Fulbright & Jaworski, LLP

M. James Daley
Redgrave Daley Ragan & Wagner LLP

Jonathan A. Damon
LeBeouf, Lamb, Greene & MacRae

Chirstopher M. Davis
Steptoe & Johnson LLP

Martha Dawson
K&L Gates

Robert J. C. Deane
Borden Ladner Gervais LLP

Daniel T. DeFeo
The DeFeo Law Firm, PC

John Paul Deley
Energy Information Administration
Observer

Jonathan E. DeMay
Condon & Forsyth LLP

Radi Dennis
Sentry Consulting Group

William B. Dodero
Bayer Corporation

Manuel J. Dominguez
Berman Devalerio Pease Tabacco Burt & Pucillo

Paul F. Doyle
Proof Space

Phillip J. Duffy
Gibbons P.C.

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

Peg Duncan
Department of Justice, Canada
Observer

Victoria Edelman
LexisNexis Applied Discovery

Deborah Edwards
Duke Energy Corporation

Elizabeth F. Edwards
McGuireWoods LLP

Robert A. Eisenberg
Capital Legal Solutions

Laura E. Ellsworth
Jones Day

Todd Elmer
H5

Amor A. Esteban
Shook Hardy & Bacon LLP

Eric J. Evain
Connolly Bove Lodge & Hutz LLP

Cameron J. Evans
Honigman Miller Schwartz and Cohn, LLP

Hon. John M. Facciola
United States District Court
District of Columbia
Observer

Mary Faria
Altria Corporate Services, Inc.

Jeffrey C. Fehrman
Electronic Evidence Labs

Joan E. Feldman
Navigant Consulting Inc.

Steve Fennell
Steptoe & Johnson LLP

Carmen Oveissi Field
Daylight Forensic & Advisory LLC

Kenneth Fields
Superior Court of AZ
Observer

Eric R. Finkelman
Ciba Specialty Chemicals Corporation

Jeffrey Flax
Administrative Office of the U.S. Courts
Observer

Jason B. Fliegel
Mayer Brown Rowe & Maw LLP

Joseph E. Foster
Akerman Senterfitt

Thomas Freeman
Reed Smith LLP

Amy Freestone
Faegre & Benson LLP

Eric M. Freidberg
Stroz Friedberg LLC

Suzanne Frost
Faegre & Benson LLP

Thomas E. Gaeta
Navigant Consulting Inc.

Randy Gainer
Davis Wright Tremaine LLP

David J. Galbenski
Lumen Legal

James H. Gallegos
Burlington Northern and Santa Fe Railway

Victoria B. Garcia
New Mexico State Court System
Observer

Aaron Gardner
Paul, Weiss, Rifkind, Wharton & Garrison LLP

Daniel K. Gelb
Gelb & Gelb LLP

Anthony I. Giacobbe Jr.
Zeichner Ellman & Krause LLP

Stanley M. Gibson
Jeffer Mangels Butler & Marmaro LLP

Daniel C. Girard
Girard Gibbs LLP

Edward Glynn
PricewaterhouseCoopers LLP

Dean Gonsowski
Xiotech, Inc.

Working Group Members & Observers cont.

James E. Gordon
Navigant Consulting Inc.

Ross Gotler
Paul, Weiss, Rifkind, Wharton & Garrison LLP

Richard Graham
Pension Benefit Guaranty Corporation
Observer

Ronald J. Green
Bank of America

Jay E. Grenig
Marquette University Law School

Ashley Griggs
Electronic Evidence Discovery, Inc.

Joseph P. Guglielmo
Whatley Drake & Kallas LLC

Matthew Hagarty
America Online, Inc.

Brian Hail
Haynes & Boone LLP

David H. Haines
Exterro

Julie Anne Halter
K&L Gates

Lori A. Ham
Poyner & Spruill LLP

Jennifer Hamilton
Deere & Company

Daniel J. Harbison
Connolly Bove Lodge & Hutz LLP

Earl Harcrow
Haynes & Boone LLP

Matthew S. Harman
King & Spalding LLP

Sherry B. Harris
Hunton & Williams LLP

Hope Haslam
Merrill Lextranet

Jeff Hatfield
Jordan Lawrence Group

Kris Haworth
LECG

Ronald J. Hedges
Nixon Peabody

Michael Henga
Pillsbury Winthrop Shaw Pittman LLP

Peter C. Hennigan
Faegre & Benson LLP

William Herr

Michael Heyrich
Citigroup Inc.

Josephine H. Hicks
Parker Poe Adams & Beinstein

Cathy Hilf
McGuireWoods LLP

Ted S. Hiser
Jones Day

Julie Hoff
Redgrave Daley Ragan & Wagner LLP

W. Michael Holm
Womble Carlyle Sandridge & Rice PLLC

Tim Hood
Redgrave Daley Ragan & Wagner LLP

Virginia W. Hoptman
Womble Carlyle Sandridge & Rice PLLC

Steve Horvath
Zantaz Inc.

Karen Hourigan
Redgrave Daley Ragan & Wagner LLP

Kelly Hoversten
Gray Plant Mooty

Geoffrey M. Howard
Bingham McCutchen LLP

Oleh Hrycko
H & A Computer Forensics

Kenton J. Hutcherson
The Hutcherson Law Firm

David W. Ichel
Simpson Thacher & Bartlett LLP

David A. Irvin
Womble Carlyle Sandridge & Rice PLLC

Conrad Jacoby
Attorney & Consultant

John Janes
Deloitte

Harvey Jang
Symantec Corp.

William R. Jenkins Jr.
Jackson Walker, LLP

John H. Jessen
Electronic Evidence Discovery, Inc.

Kevin F. Joerling
ARMA International

Monica Johnson
Faegre & Benson LLP

Mary Jo Johnson
Wilmer Cutler Pickering Hale and Dorr LLP

Appendix C

Working Group Members & Observers cont.

Glenn Johnson
King & Spalding LLP

Deborah A. Johnson
Orchestria

Jeffrey J. Joyce
Jones Day

Deborah Juhnke
Blackwell Sanders Peper Martin LLP

Randolph A. Kahn
Kahn Consulting Inc.

Sidney Kanazawa
Van Etten Suzumoto & Becket LLP

Dr. Hironao Kaneko
Tokyo Institute of Technology

Larry Kanter
Alvarez & Marsal

Gregory S. Kaufman
Sutherland Asbill & Brennan

Conrad S. Kee
Jackson Lewis LLP

Gaither Keener Jr.
Lowe's Companies, Inc.

John B. Kennedy
LeBeouf, Lamb, Greene & MacRae

Anne Kershaw
A. Kershaw PC, Attorneys and Consultants

Priya Keshav
Tusker Group LP

David J. Kessler
Drinker Biddle & Reath LLP

Laura M. Kibbe
Pfizer Inc.

Elizabeth Kidd
LexisNexis Applied Discovery

Dennis Kiker
Moran Kiker Brown PC

John K. Kim
Johnson & Johnson

Mike Kinnaman
Attenex Corporation

Shannon Capone Kirk
Ungaretti & Harris

David Kittrell

Gene Klimov
DOAR Litigation Consulting

Melissa L. Klipp
Drinker Biddle & Reath LLP

Liane R. Komagome
Hewlett Packard

Steven S. Krane
Barton Barton & Plotkin LLP

Antigone Kriss
Chambers of Judge Kimberly Moore
Observer

K. J. Kuchta
Forensics Consultation Solutions, LLC

James S. Kurz
Womble Carlyle Sandridge & Rice PLLC

Bradley R. Kutrow
Helms Mulliss & Wicker

Janet Kwuon
Reed Smith LLP

Francis Lambert
Zantaz Inc.

Edwin M. Larkin
Winston & Strawn LLP

Monica Wiseman Latin
Carrington, Coleman, Sloman & Blumenthal, L.L.P.

Brandon Lee
Deloitte Financial Advisory Services LLP

R. Michael Leonard
Womble Carlyle Sandridge & Rice PLLC

Ronald J. Levine
Herrick Feinstein LLP

Pauline Levy
McDonalds Corporation

Robert Levy
Haynes & Boone LLP

Paul Lewis
Protiviti

Julie Lewis
Digital Mountain, Inc.

Thomas Lidbury
Mayer, Brown, Rowe & Maw LLP

Joe Looby
FTI

Ralph Losey
Akerman Senterfitt

Lorrie L. Luellig
Ryley Carlock & Applewhite

Patricia Clarke Lukens

James K. Lynch
Latham & Watkins LLP

Appendix C

Working Group Members & Observers cont.

Cecil Lynn
LexisNexis Applied Discovery

Sheila Mackay
Daegis

Audra Hale Maddox
Womble Carlyle Sandridge & Rice PLLC

Heidi Maher
Renew Data Corp.

Michelle Mahoney
Mallesons Stephen Jaques

Sheri Malec
McDonalds Corporation

Carrie Mallen
McKesson Corporation

A. John P. Mancini
Mayer Brown Rowe & Maw LLP

Joseph Mann
Merrill Lextranet

Browning E. Marean III
DLA Piper

Robert Markham
Cohasset Associates, Inc.

David G. Martin
Medtronic, Inc.

James H. Martin
Office of the Attorney General of New Jersey
Observer

Ann Marie Mason
Metropolitan Life Insurance Co.

Geoffry C. Mason
Sidley Austin LLP

Kathleen M. Massey
Motorola Inc.

J. W. Matthews III
Haynesworth Sinkler Boyd, P.A.

Wayne Matus
Mayer Brown Rowe & Maw LLP

Tom Matzen
Xact

J. J. McCracken
Cooper Tire & Rubber Company

Anne B. McCray
McGuireWoods LLP

Gregory McCurdy
Microsoft Corporation

Nancy McMahon
Department of Justice
Observer

William McManus
Ryley Carlock & Applewhite

Stephanie Mendelsohn
Genentech

James L. Michalowicz
ACT Litigation Services

Lucie Miller
Eli Lilly & Co.

Bill Millican
ARMA International

Scott Milner
Morgan Lewis & Bockius LLP

Denise M. Mineck
Life Investors Insurance Company of America

Robert D. Moody
Berenfeld, Spritzer, Shechter & Sheer

Tim Moorehead
BP America, Inc.

Jack Moorman
PricewaterhouseCoopers LLP

Steve Morrissett
Finnegan Henderson Farabow Garrett & Dunner LLP

Helen Bergman Moure
K&L Gates

Shelia Murphy
Metropolitan Life Insurance Co.

Justin Myers
Rambus

Simon Nagel
Dechert LLP

Paul J. Neale Jr.
DOAR Litigation Consulting

Jon A. Neiditz
Lord Bissell & Brook LLP

John Nemazi
Brooks Kushman PC

Mollie Nichols
First Advantage

Jonathan Nystrom
Cataphora

John Oakley
Berenfeld, Spritzer, Shechter & Sheer

Kate O'Brien
Digital Mandate

Kate Oberlies O'Leary
General Electric Company

Timothy L. O'Mara
Latham & Watkins LLP

Maureen O'Neill
Paul, Hastings, Janofsky & Walker, LLP

Appendix C

Working Group Members & Observers cont.

Patrick Oot
Verizon Communications

Timothy M. Opsitnick
JurInnov Ltd.

Greg Osinoff
Digital Mandate

Robert D. Owen
Fulbright & Jaworski, LLP

Laura Lewis Owens
Alston & Bird, LLP

Neil Packard
e-Diligent, Inc.

Deidre Paknad
PSS Systems Inc.

Robert W. Pass
Carlton Fields

Thomas Pasternak
DLA Piper

John Patzakis
Guidance Software

George L. Paul
Lewis & Roca LLP

Richard Pearce-Moses
Arizona State Library
Observer

Cheryl L. Pederson
Cargill Inc.

Peter Pepiton II
CA Inc.

Ginger Heyman Pigott
Reed Smith LLP

Justin David Pitt
Bass, Berry & Sims PLC

Jeanette Plante
U.S. Department of Justice, Justice Management Divison, Office of Records Mangement Policy
Observer

Vivian Polak
LeBeouf, Lamb, Greene & MacRae

Anthony Polk
Electronic Evidence Discovery, Inc.

Ashish S. Prasad
Mayer Brown Rowe & Maw LLP

James Proscia
Brooks Kushman PC

Michael J. Prounis
Evidence Exchange

Charles R. Ragan
Redgrave Daley Ragan & Wagner LLP

Sreenu P. Raju
Sreenu P. Raju, P.L.C.

Donald C. Ramsay
Stinson Morrison Hecker LLP

Jonathan Redgrave
Redgrave Daley Ragan & Wagner LLP

Jeffrey Reed
Maron & Marvel PA

Heather Reed
Capital One Services, Inc.

Daniel L. Regard
LECG

Mark V. Reichenbach

Anthony Reid
Deloitte Financial Advisory Services LLP

David Remnitz
FTI

Ann Marie Riberdy
Wilmer Cutler Pickering Hale and Dorr LLP

Mark (Rick) E. Richardson III
Glaxo Smith Kline

Mary K. Riley
Bank of America

John T. Ritter
Bank of America

Karin A. Roberts
Eli Lilly & Co.

Paul M. Robertson
Redgrave Daley Ragan & Wagner LLP

William C.E. Robinson
GEICO Insurance Company

E. Casey Roche III
Discovery Mining Inc.

Michael S. Roe
Ashland Inc.

Dave Rogers
Ernst & Young LLP

Herbert L. Roitblat
Orcatec LLC

James E. Rooks Jr.
Association of Trial Lawyers of America

Andrea D. Rose
Crowell & Moring LLP

John J. Rosenthal
Howery LLP

Hon. Lee H. Rosenthal
United States District Court
Southern District of Texas
Observer

Appendix C

Working Group Members & Observers cont.

Ira P. Rothken
Rothken Law Firm

Charles Rothman
H & A Computer Forensics

Kenneth Rowe
Chief Security Officers

Ashley Rowe
Metlife

Jane K. Rushton

Stuart K. Sammis
Corning Incorporated

Joseph R. Saveri
Lieff Cbraser Heimann & Bernstein, LLP

Leigh R. Schachter
Verizon Wireless

Gregory P. Schaffer
Alltell Corporation

Karen Schak
Deloitte

Hon. Shira A. Scheindlin
United States District Court
Southern District of New York
Observer

David Schieferstein
Philip Morris U.S.A

Ryan Schmelz
Riberian Enterprises Inc.

Christopher Schnabel
Paul, Weiss, Rifkind, Wharton & Garrison LLP

Eric J. Schwarz
Ernst & Young LLP

Dan P. Sedor
Jeffer Mangels Butler & Marmaro LLP

P. Brian See
Seyfarth Shaw LLP

Steven Shankroff
Skadden ARPS

Jeffrey C. Sharer
Sidley Austin LLP

Jackson Sharman III
Lightfoot Franklin & White

Kenneth Shear

Gregory Shelton
Williams Kastner & Gibbs PLLC

Robert W. Shely
Bryan Cave LLP

James D. Shook
EMC Corporation

Mark Sidoti
Gibbons P.C.

Sonya L. Sigler
Cataphora

Tom J. Sikora
El Paso Corporation

Dominique Simard
Ogilvy Renault LLP

Robert R. Simpson
Shipman & Goodwin LLP

Julie Sinor
PricewaterhouseCoopers LLP

Amy Sipe
ACT Litigation Services

Peter B. Sloan
Blackwell Sanders Peper Martin LLP

Thomas J. Smedinghoff
Wildman, Harrold LLP

Arthur L. Smith
Husch & Eppenberger

Jessica Cullen Smith
McDermott Will & Emery

Howard Smith
Barton Barton & Plotkin LLP

Ken Sokol
Electronic Evidence Discovery, Inc.

Catherine J. Sosso
Union Pacific Railroad Company

Carolyn Southerland
Baker Botts LLP

Judith Starr
Pension Benefit Guaranty Corporation
Observer

Stephen R. Stegich III
Condon & Forsyth LLP

Heidi Stenberg
Ernst & Young LLP

Kimberly Baldwin Stried
KBS Consulting - Lake County Physicians Association

Cheryl Strom
McDonalds Corporation

Ariana J. Tadler
Milberg Weiss Barshad & Schulman LLP

Appendix C

Working Group Members & Observers cont.

Steven W. Teppler
Steven W. Teppler, Esq.

Jeane Thomas
Crowell & Moring LLP

Paul Thompson
Dartmouth College

Hon. Samuel A. Thumma
Maricopa County Superior Court
Observer

Christina (Tina) Torres
Microsoft Corporation

Robert W. Trenchard
Wilmer Cutler Pickering Hale and Dorr LLP

John Turner
AnaComp

Judy Van Dusen
VanKorn Group, Limited

Jason Velasco

A. J. Venit
Bank of America

Peter Wacht
National Court Reporters Association

Jim Wagner
DiscoverReady

Lori Ann Wagner
Redgrave Daley Ragan & Wagner LLP

Vincent Walden
Ernst & Young LLP

Kathryn Hannen Walker
Bass, Berry & Sims PLC

Alston Walker
Stroock & Stroock & Lavan LLP

Skip Walter
Attenex Corporation

Paul L. Warner
Jeffer Mangels Butler & Marmaro LLP

Hon. Ira B. Warshawsky
Supreme Court of New York, Commercial Division
Observer

Ryan Wasell
Weyerhaeuser Company

Emroy Watson
Yamaha Motor Corporation

Hon. David Waxse
United States District Court
District of Kansas
Observer

Laurie A. Weiss
Fulbright & Jaworski, LLP

Brian Westenberg
Daimler Chrysler Corp.

David Wetmore
Ernst & Young LLP

Maggie Whitney
Sidley Austin LLP

Robert B. Wiggins
Morgan Lewis & Bockius LLP

James "Chuck" Williams
MetaLINCS

Jack Williams
Powell, Goldstein, Frazer & Murphy

Robert F. Williams
Cohasset Associates, Inc.

Scott L. Winkelman
Crowell & Moring LLP

Thomas P. Wisinski
Haynes & Boone LLP

Kenneth J. Withers
The Sedona Conference
Ex Officio

Edward C. Wolfe
General Motors Corporation

Gregory B. Wood
Fulbright & Jaworski, LLP

Todd I. Woods
Lowe's Companies, Inc.

Sarah E. Worley
Pre-Trial Solutions, Inc.

Susan B. Wortzman
Lerners LLP

Joel Wuesthoff
Ibis Consulting

Chris Yowell
Celerity Consulting

Jason Yurasek
Bingham McCutchen LLP

Patrick Zeller
Guidance Software

The Sedona Conference Working Group Series & WGS℠ Membership Program

"DIALOGUE DESIGNED TO MOVE THE LAW FORWARD IN A REASONED AND JUST WAY."

The Sedona Conference® Working Group Series ("WGS℠") represents the evolution of The Sedona Conference® from a forum for advanced dialogue to an open think-tank confronting some of the most challenging issues faced by our legal system today.

The WGS℠ begins with the same high caliber of participants as our regular season conferences. The total, active group, however, is limited to 30-35 instead of 60. Further, in lieu of finished papers being posted on the website in advance of the Conference, thought pieces and other ideas are exchanged ahead of time, and the Working Group meeting becomes the opportunity to create a set of recommendations, guidelines or other position piece designed to be of immediate benefit to the bench and bar, and to move the law forward in a reasoned and just way. Working Group output, when complete, is then put through a peer review process, including where possible critique at one of our regular season conferences, hopefully resulting in authoritative, meaningful and balanced final papers for publication and distribution.

The first Working Group was convened in October 2002, and was dedicated to the development of guidelines for electronic document retention and production. The impact of its first (draft) publication—*The Sedona Principles; Best Practices Recommendations and Principles Addressing Electronic Document Production* (March 2003 version)—was immediate and substantial. *The Principles* was cited in the Judicial Conference of the United State Advisory Committee on Civil Rules Discovery Subcommittee Report on Electronic Discovery less than a month after the publication of the "public comment" draft, and was cited in a seminal e-discovery decision of the Federal District Court in New York less than a month after that. As noted in the June 2003 issue of Pike & Fischer's *Digital Discovery and E-Evidence, "The Principles*...influence is already becoming evident."

The WGS℠ Membership Program was established to provide a vehicle to allow any interested jurist, attorney, academic or consultant to participate in Working Group activities. Membership provides access to advance drafts of Working Group output with the opportunity for early input, and to a Bulletin Board where reference materials are posted and current news and other matters of interest can be discussed. Members may also indicate their willingness to volunteer for special Project Team assignment, and a Member's Roster is included in Working Group publications.

We currently have active Working Groups in the areas of 1) electronic document retention and production; 2) protective orders, confidentiality, and public access; 3) the role of economics in antitrust; 4) the intersection of the patent and antitrust laws; (5) *Markman* hearings and claim construction; (6) international e-information disclosure and management issues; and (7) e-discovery in Canadian civil litigation. *See* the "Working Group Series" area of our website www.thesedonaconference.org for further details on our Working Group Series and the WGS℠ Membership Program.

Visit www.thesedonaconference.org