404 Leading Through the Electronic Discovery Quagmire (Part 2): Current Case Law & Practical Considerations

Michael R. Arkfeld
Attorney, Author and Consultant
Arkfeld & Associates

Mollie Nichols
Senior Vice President and General Counsel
First Advantage Litigation Consulting

Honorable Shira Ann Scheindlin
Judge
United States District Court

Faculty Biographies

Michael R. Arkfeld

Michael R. Arkfeld is a consultant engaged in speaking, writing, and consulting on a wide variety of issues regarding electronic discovery and evidence at Arkfeld & Associates in Phoenix.

Prior to his consulting and writing career, Mr. Arkfeld was employed as an assistant United States attorney for the District of Arizona specializing in civil tort litigation. He has appeared before both federal and state appellate courts and has extensive experience in jury (over 30 trials) and bench trials. Mr. Arkfeld has presented as a keynote speaker, conference presenter, and trainer at over 200 conferences throughout North America and internationally on the impact of technology to the practice of law, and on discovery and admission of electronic evidence.

Mr. Arkfeld is the author of one of the leading e-discovery treatises in the country - Electronic Discovery and Evidence and was the recipient of the e-evidence thought leading scholar award.

Mollie Nichols

Mollie C. Nichols, is senior vice president and counsel for First Advantage, litigation consulting services division in Chantilly, Virginia. Ms. Nichols has experience as a litigator, a law professor, and a litigation consultant in both civil and criminal litigation working for the federal and state government and in private practice.

She was formerly the associate director for research and professional development for the Courtroom 21 Project.

Ms. Nichols is a member of ACC's Litigation Committee. She teaches digital discovery and evidence at William & Mary Law School, as an adjunct professor. She also lectured at the University of Texas McCombs School of Business on legal topics including the protection and security of information systems. Ms. Nichols is a frequent speaker at continuing legal education programs on electronic discovery and litigation preparedness topics and has authored articles on topics including electronic discovery, courtroom technology, and global encryption policies.

She received her Doctor of Jurisprudence and Masters of Law from the University of Texas School of Law.

Honorable Shira Ann Scheindlin

The Honorable Shira A. Scheindlin is United States district judge for the Southern District of New York. She is also an adjunct professor at Brooklyn Law School.

Previously, she was law clerk to the Hon. Charles Brieant, Jr. of the United States District Court for the Southern District of New York, assistant United States attorney for the Eastern District of New York, general counsel to the New York City Department of Investigation, United States magistrate judge for the United States District Court for the Eastern District of New York, member of the civil justice reform act advisory group Southern District of New York, chair of the grievance committee of the Southern District of New York, and a member of the judicial conference of the United States advisory committee on the Federal Rules of Civil Procedure.

She is a member of the American Law Institute, New York County Lawyer's Association, Association of the Bar of the City of New York, Federal Bar Council, New York State Bar Association, New York State Bar Foundation, Justice Resource Center, Cornell Law School Advisory Council, Good Shepherd Services, Sedona Conference, and the New York Inn of Court. Judge Scheindlin has received the United States Department of Justice Special Achievement Award, the New York State Bar Association Haig Award, the New York State Bar Association Brennan Award, and the New York County Lawyer's Association Weinfeld Award.

She received her B.A. from the University of Michigan, M.A. from Columbia University, and J.D. from Cornell Law School.

Guiding Your Electronic Discovery and Evidence Decisions

Prepared for:

Association of Corporate Counsel
Tuesday, Oct 24, 9:00 AM - 10:30 AM.
San Diego, CA

Leading Through the Electronic Discovery Quagmire (Part 2): Current Case Law & Practical Considerations

Emerging Trends in E-Discovery

By

Michael R. Arkfeld, Esq.

* * * * * * * *

- **Contact Information: Michael@arkfeld.com**
- **Author: *Electronic Discovery and Evidence treatise* and *The Digital Practice of Law* (available at www.lawpartnerpublishing.com);**
- **For other articles, daily comments and materials on electronic discovery and evidence visit the following companion web sites:**
  - **The Electronic Discovery and Evidence Blog (http://arkfeld.blogs.com/ede/)**
  - **Free electronic discovery newsletter (www.lawpartnerpublishing.com)**

9602 North 35th Place
Phoenix, AZ
85028

Ph: 602-380-7488
E-mail: Michael@arkfeld.com
Fax: 866-617-0736
Web site: www.arkfeldandassociates.com

Emerging Trends in E-Discovery Law

by

Michael R. Arkfeld

Author: Michael R. Arkfeld is a practicing attorney, speaker and author. Michael is the author of the *Electronic Discovery and Evidence* treatise (updated August 2006), *E-Discovery Best Practices Guide* and *The Digital Practice of Law* (5th ed.) available at Law Partner Publishing, LLC (www.lawpartnerpublishing.com). He is a member of the State Bar of Arizona and the recipient of the national 2004 E-Evidence Thought Leading Scholar Award. His web sites at www.arkfeld.com and www.arkfeldandassociates.com feature additional electronic discovery and evidence materials and other resources. He can be reached at Michael@arkfeld.com.

I. The Duty to Preserve and Disclose Metadata.

Introduction to metadata

What is metadata?

Metadata is information used by the computer to manage and often classify the computer file from which it originated. *Madison River Mgmt. Co. v. Business Mgmt. Software Corp.*, 387 F. Supp. 2d 521, 528 n.5 (D.N.C. 2005) ("[m]etadata means, literally, data about data. It describes 'how and when and by whom a particular set of data was collected, and how the data is formatted.'"). Metadata is "embedded" information that is stored in electronically generated materials, but which is not visible when a document or materials are printed.

ABA Civil Discovery Standards, § 29(b)(ii)(B) contains this description of metadata: "A party requesting information in electronic form should also consider . . . [a]sking for the production of metadata associated with the responsive data - i.e., ancillary electronic information that relates to responsive electronic data, such as information that would indicate whether and when the responsive electronic data was created, edited, sent, received and/or opened."

There are two types of metadata that are maintained by a computer system about a particular computer file, "file system" and "embedded" metadata. Computer logs are often described as "metadata" about the computer system in use.

Metadata - specific file format

- Text document
- Spreadsheet
- E-mail
- Others

Viewing metadata

- E-Discovery software - extract
- Import into a database program such as Summation or Concordance

Legal Issues

Authentication evidence - Fed. R. Evid. 104, 901

- *Krumwiede v. Brighton Associates, L.L.C.*, No. CIV.05-3003, 2006 WL 1308629 (N.D. Ill. May 8, 2006).

Best evidence - Fed. R. Evid. 1001

Direct or circumstantial evidence

- *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640 (D. Kan. 2005). The Court ordered an employer in an employment discrimination case to restore the metadata it had "scrubbed" or "erased" from Excel spreadsheet files and "unlock" them.

Privilege and ethical issues

- Attorney client, work product, trade secrets
- Data mining - ethical or unethical?
- *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640 (D. Kan. 2005). The Court found that since the employer had failed to provide a privilege log for the electronic documents it claimed contained metadata that would reveal privileged communications, it waived any privilege.

Regularly maintained

- *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 656-657 (D. Kan. 2005). "When the Court orders a party to produce an electronic document in the form in which it is regularly maintained, i.e., in its native format or as an active file, that production must include all metadata unless that party timely objects to production of the metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order." (emphasis added).

Court rules

> *District of Delaware* – local rule
>
> Default Standard for Discovery of Electronic Documents ("E-Discovery")
>
> 6. Format. If, during the course of the Rule 26(f) conference, the parties cannot agree to the format for document production, electronic documents shall be produced to the requesting party as image files (e.g., PDF or TIFF). When the image file is produced, the producing party must preserve the integrity of the electronic document's contents, i.e., the original formatting of the document, its metadata and, where applicable, its revision history. After initial production in image file format is complete, a party must demonstrate particularized need for production of electronic documents in their native format.

Pending Federal Rule - Rule 26(f), Committee Note.

> "These problems often become more acute when discovery of electronically stored information is sought. The volume of such data, and the informality that attends use of e-mail and some other types of electronically stored information, may make privilege determinations more difficult, and privilege review correspondingly more expensive and time consuming. Other aspects of electronically stored information pose particular difficulties for privilege review. For example, production may be sought of information automatically included in electronic files but not apparent to the creator or to readers. Computer programs may retain draft language, editorial comments, and other deleted matter (sometimes referred to as "embedded data" or "embedded edits") in an electronic file but not make them apparent to the reader. Information describing the history, tracking, or management of an electronic file (sometimes called "metadata") is usually not apparent to the reader viewing a hard copy or a screen image. Whether this information should be produced may be among the topics discussed in the Rule 26(f) conference. If it is, it may need to be reviewed to ensure that no privileged information is included, further complicating the task of privilege review."

Redaction and Bate-stamp issues

- *Hagenbuch v. 3B6 Sistemi Elettronici Industriali* S.R.L., 2006 W.L. 665005 (N.D. Ill. Mar. 8, 2006). The Court ordered the defendant to produce electronic information in native file format instead of the TIFF format that the defendant desired. The defendant argued that production in a TIFF format would allow it to produce the data with bates labeling and to protect confidential or privileged information. The Court rejected the position observing that TIFF production does not contain "the creation and modification dates of a document, e-mail attachments and recipients, and metadata" which was possibly relevant to plaintiff's case as it could relate to the chronology of events and "who received what information and when."

Since metadata may provide direct or circumstantial evidence, authentication and may be the Best Evidence, its discovery will become commonplace.

II. The Duty to Provide a Certification of the Search Protocol.

What is a search protocol certification?

What is the scope of the protocol?

- Which computer devices and media were accessed in acquiring the data
- What search terms were utilized to gather the evidence
- What filtering rules were in effect
- What search software was used
- What keywords or other search techniques were used to acquire the data?
- What chain of custody was utilized to keep the data from being tainted?

© 2006 Michael R. Arkfeld

- Other

What certification is required?

- 26(g) - Rule 26(g)(2) requires an attorney to sign all discovery requests, responses and objections. By signing an attorney is certifying that to the "best of the signer's knowledge, information, and belief, formed after a reasonable inquiry, the request, response, or objection is: . . . (B) not interposed for any improper purpose, such as to harass or to cause unnecessary delay or needless increase in the cost of litigation. . . . (C) not unreasonable or unduly burdensome or expensive, given the needs of the case, the discovery already had in the case, the amount in controversy, and the importance of the issues at stake in the litigation." Rule 26(g)(3) provides for an "appropriate sanction, which may include an order to pay the amount of the reasonable expenses incurred because of the violation, including a reasonable attorney's fee."
- The purpose of Rule 26(g) is to create "an affirmative duty to engage in pretrial discovery in a responsible manner." Fed. R. Civ. P. 26(g) Advisory Committee Notes to 1983 Amendments. The attorney's signature is not a certification of the truthfulness of the client's responses. "Rather, the signature certifies that the lawyer has made a reasonable effort to assure that the client has provided all the information and documents available to him that are responsive to the discovery demand." Fed. R. Civ. P. 26(g) Advisory Committee Notes to 1983 Amendments. What is reasonable is a matter for the court to decide on the totality of the circumstances. Fed. R. Civ. P. 26(g) Advisory Committee Notes to 1983 Amendments. If a certification is made in violation of Rule 26(g)(3) is without "substantial justification then sanctions may be imposed."

Legal opinions (sampling of cases)

Search protocol description

- *United States v. Maali*, 346 F. Supp.2d 1226, 1264 (M.D.Fla. 2004).

Search protocol certification required

- *Convolve, Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162, 168 (S.D.N.Y. 2004).

Search protocol disregarded

- *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, No. CIV.98-827, 2005 WL 22833, at *53 n.143 (S.D.N.Y. Jan. 5, 2005).
-

Unfortunate result – failure to certify

- *Quinby v. WestLB AG*, No. CIV.04-7406, 2005 U.S. Dist. LEXIS 35583 (D.N.Y. Dec. 15, 2005).

Meet and confer to determine search protocol

- *Treppel v. Biovail Corp.*, 233 F.R.D. 363, 373-374 (D.N.Y. 2006).

Court rule

- Local rule - Eastern and Western Districts of Arkansas Local Civil Rule 26.1: "5. Search methodology. If the parties intend to employ an electronic search to locate relevant electronic documents, the parties shall disclose any restrictions as to scope and method which might affect their ability to conduct a complete electronic search of the electronic documents. The parties shall reach agreement as to the method of searching, and the words, terms, and phrases to be searched with the assistance of the respective e-discovery liaisons, who are charged with familiarity with the parties' respective systems. The parties also shall reach agreement as to the timing and conditions of any additional searches which may become necessary in the normal course of discovery. To minimize the expense, the parties may consider limiting the scope of the electronic search (e.g., time frames, fields, document types)."

Other Authorities

- Jason R. Baron, *Toward a Federal Benchmarking Standard for Evaluating Information Retrieval Products Used in E-Discovery*, 6 Sedona Conf. J. 237 (2005).

The certification of the identification, preservation and collection protocol will become a routine part of discovery.

III. The Duty to Provide Electronic Data as it is "Kept in the Regular Course of Business," "In a Reasonably Usable Format," and "In a Mutually Agreed Upon Format."

Kept in the Usual Course of Business

- Fed. R. Civ. P. 34 - Production of Documents. Rule 34(a) states: "(a) Scope. Any party may serve on any other party a request (1) to produce . . . to inspect and copy, any designated documents . . . and other data compilations from which information can be obtained. . . . or to inspect and copy, test, or sample any tangible things which constitute or contain matters within the scope of Rule 26(b). . . ." This rule permits, under certain circumstances, inspection of opposing party's computer system and for the forensic copy of storage media such as a hard drive. In addition, the Rule provides they shall be produced "*as they are kept in the usual course of business . . .* " (emphasis added).

- *Jackson v. City of San Antonio*, No. CIV.03-0049, 2006 U.S. Dist. LEXIS 8091 (W.D. Tex., Jan. 31, 2006).

Translated Into Reasonably Useful Form

- Fed. R. Civ. P. 34 advisory committee notes (1970 amendments). Rule 34 permits the discovery of any "documents" and *"data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably useful form."* (emphasis added).
- *Powerhouse Marks, L.L.C. v. Chi Hsin Impex*, Inc., No. CIV.04-73923, 2006 U.S. Dist. LEXIS 2767, at *9-11 (D. Mich. Jan. 12, 2006).

Pending Rule 34 Amendment

- The pending Rule 34(b) Amendment Committee Note recognizes that: "Rule 34(b) provides that a party must produce documents as they are kept in the usual course of business or must organize and label them to correspond with the categories in the discovery request." "If the form of production is not specified by party agreement or court order, the responding party must produce electronically stored information either in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable." "Rule 34(a) requires that, if necessary, a responding party "translate" information it produces into a "reasonably usable" form."

Mutually agreed upon form

- § 7.07[A][1], Pending Rule 34 Amendment. The pending Rule 34 expands the scope to include "electronically stored information . . . The request may specify the form or forms in which electronically stored information is to be produced. . . . The response shall include "an objection to the requested form or forms for producing electronically stored information, stating the reasons for the objection. . . . 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 objection is made to part of an item or category, the part shall be specified and inspection permitted of the remaining parts. . . .
- The party submitting the request may move for an order under Rule 37(a) with respect to any objection to or other failure to respond to the request or any part thereof, or any failure to permit inspection as requested. . . .
- If a party in their request "does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable; and . . . a party need not produce the same electronically stored information in more than one form."

The format protocol for the disclosure of electronic discovery will become more "standardized" as litigants begin to understand electronic data and apply the Federal Rules of Civil Procedure.

IV. The Courts will become increasing frustrated by legal professionals who lack the necessary knowledge to handle electronic discovery.

Lawyers and their clients

- Michael A. Clark, *EDD Supplier Landscape, Electronic Discovery in Litigation Series*, October 28, 2004. When suppliers were asked "[w]hat percentage of AmLaw 200 firms has the requisite knowledge and experience to professionally handle a complex EDD matter?" There was a broad consensus that the answer was not more than 25%.

- "[I]n a 2000 American Bar Association membership survey, 83 percent of the respondents said that their corporate clients had no established protocol to deal with discovery requests for electronic data." Ashby Jones, "*What a Mess!, For Corporations, Pileup of Electronic Data Could Be Trouble Waiting to Happen,"* National Law J. (Dec. 2, 2002) at C6. "This problem is compounded by the fact that many in-house lawyers 'are very uncomfortable' with the technical aspects of document management." *Id.* at C7.

Ethical Rules

- ABA Model Rule of Professional Conduct 1.1 provides that "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."
- ABA Model Rule of Professional Conduct 1.3 provides that "A lawyer shall act with reasonable diligence and promptness in representing a client."
- ABA Model Rule of Professional Conduct 1.6 provides that "(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent . . ."
- ABA Model Rule of Professional Conduct 3.4(a) provides that "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 [and] . . . shall not counsel or assist another person to do any such act. . . ."
- ABA Model Rule of Professional Conduct 8.4(c)-(d) proscribes "dishonesty, fraud, deceit, or misrepresentation [or] conduct that is prejudicial to the administration of justice."

Legal Opinions

- *Danis v. USN Communications, Inc.*, No. CIV.98-7482, 2000 WL 1694325, at *1 (N.D. Ill. Oct. 20, 2000) the Court stated: "The duty of disclosure finds expression not only in the rules of discovery, but also in this Court's Rules of Professional Conduct, which prohibit an attorney from 'suppress[ing] any evidence that the lawyer or client has a legal obligation to reveal or produce,' Rules for the Northern District of Illinois, LR 83.53.3(a)(13), or from 'unlawfully obstructing another party's access to evidence . . . Id. LR 83.53.4(1)."

- *Metropolitan Opera Ass'n., Inc. v. Local 100*, 212 F.R.D. 178, 181, 222-223, 231 (S.D.N.Y. 2003), *adhered to on reconsideration*, 2004 WL 1943099 (S.D.N.Y. Aug. 27, 2004). The Court found liability against the defendant and noted that defendants' lawyers "completely abdicated their responsibilities under the discovery rules and as officers of the court" and defendants "lied and, through omission and commission, failed to search for and produce documents and, indeed, destroyed evidence--all to the ultimate prejudice of the truth-seeking process."

- *TIG Insurance Co. v. Giffin Winning Cohen & Bodewes*, P.C., 2006 WL 890763 (7th Cir. April 7, 2006). An insurance company brought a malpractice claim against a law firm claiming that it was negligent in the untimely production of electronic information (gender equity studies) in the underlying employment cases. The Court eventually held that the damages of 1.2 million dollars for legal fees paid to another firm for defending against sanctions was not reasonably foreseeable.

The Courts will continue to impose sanctions on attorneys who fail to properly discover, preserve and produce electronic discovery.

the wired lawyer | BY MICHAEL R. ARKFELD

Electronic Discovery Here to Stay

How many of you have sought to discover and admit into court electronic information from an opposing party? In my informal polls few of you can answer this question in the affirmative. However, this is an extremely important litigation issue and will increase in importance.

The world has changed. Now, millions of e-mails are sent daily; a typical person receives more than 30 a day. Drafts and redrafts of important business and other word processing documents are viewed and commented upon by many people and stored on computers located in many different locations. Conversations between business associates are occurring in real-time with instant messaging. Many individuals and businesses use individual or joint calendars. Many documents, data and other electronic materials are no longer being converted to paper but are created, revised and stored in electronic format. Because of this, it is necessary to "discover" this electronic information in your cases.

Would it assist you to:

- View the e-mail of an opposing party who corresponds with other people about the details of his or her accident and alleged injuries?
- Obtain e-mail or other electronic evidence from an employer who has been sexually harassing an employee?
- Read the e-mail between the owner, employees or customers in a business dispute case?
- Read drafts of documents or internal memoranda that discuss the opposing business party's strategy to unfairly compete against your client's services or products?

Most cases probably contain electronic information from the opposing party that is relevant and discoverable in your case. But if you have access to the paper discovery, why discover electronic information?

Because electronic information is different and in many ways contains information of greater value than analog or paper information.

1. Creation of electronic information is often made without concern as to formality or an understanding that it can be later discovered—as seen in the Microsoft antitrust trial.
2. Drafts and redrafts of electronic documents often can be discovered. Both Microsoft Word and WordPerfect have features that allow prior drafts of word processing documents to be recovered and viewed.
3. Metadata or "imbedded data" is often contained in electronic files that allows you to view the author, persons who viewed the document and changes made to the document.
4. Electronic evidence is more easily deleted, destroyed or altered. But "deleted" information may be "undeleted" and files opened and viewed—and the information may not have been deleted from all computers.
5. Once "discovered," electronic information can be searched by word, phrase or date. If you obtain electronic information through discovery, it usually is in a full-text format that lends itself to be searched via software.
6. Whereas paper documents are usually located in certain files and file cabinets, electronic information can be stored in many different formal and informal locations in a computer system.

How electronic data are created and stored is very important. Interrogatories or discovery depositions should focus on the system the opposing party is using regarding the type of computer systems used, filing system, archival of data, destruction of e-mail, and so forth. This prevents costly discovery and needless searching of electronic information.

Finally, authentication and laying the foundation for electronic information for admissibility must be treated with extreme

Upcoming columns on electronic information will focus on:

- Discoverability and admissibility
- Court rules
- Choosing a computer forensics expert
- Software to view digital information

care. There are horror stories of IT personnel or attorneys who, after discovering electronic information, do not "open" and view the data properly and open the door for challenges to the foundation for the discovered information.

The request, production, use and admissibility of electronic information are part of a complex process. Interrogatories requesting information as to the systems and personnel responsible for electronic data must be prepared and served. Request for production or electronic replication of the electronic information must be filed requesting "copies" of "hard disks" or other storage media. A computer forensics expert is generally needed to assist in the identification and conversion of electronic information.

Unfortunately, this can be expensive, but as this discovery area matures, less costly methods will be developed to allow for discovery and admission of this information.

Michael R. Arkfeld is an Assistant United States Attorney in Phoenix. He is the author of *The Digital Practice of Law* (5th edition) and a frequent speaker and columnist on the practice of law. He can be reached at Michael@Arkfeld.com.

Electronic Discovery and Evidence

Michael R. Arkfeld

Member of the State Bar of Arizona

2005-2006 ed.
Law Partner Publishing, LLC
Phoenix * Arizona

SUMMARY OF CONTENTS

2004 - 2005 ed.

Chapter 1

Electronic Information in Litigation

§ 1.01 TRANSITION TO ELECTRONIC INFORMATION

The ubiquitous use of computers for creating electronic information has dramatically changed discovery and admission of case information. Whether in business, government or at home, information is being created in an electronic format. "According to a University of California study, 93% of all information generated during 1999 was generated in digital form, on computers. Only 7% of information originated in other media, such as paper." *In re Bristol-Myers Squibb Securities Litigation,* 205 F.R.D. 437, 440 n.2 (D.N.J. 2002). Not only is this change pervasive, it has occurred quickly.

In a short period of time technology, computers and the Internet have radically changed the way we create and transmit information. In 1975 the first microcomputer was introduced which replicated the power of larger computers into a small desktop. This breakthrough was the result of the miniaturization of new microprocessor technologies called semiconductors. These were followed by the introduction of the first word processing software in 1978, which enabled people to easily write and change text and graphics. Over the next 20 years, computers found their way into millions of households and businesses. One commentator noted, "[i]n 1991 companies for the first time spent more on computing and communications gear . . . than on industrial, mining, farm, and construction machines. Infotech is now as vital . . . as the air we breathe." Thomas A. Stewart, *The Information Age in Charts,* Fortune, April 4, 1994, at 75-79.

Coupled with the introduction of Internet, which allowed information to be transferred in an electronic format, electronic information created by computers could easily be transmitted worldwide in seconds. This combination of computers and the Internet laid the foundation for the societal change commonly known as The Digital Age, The Information Age or the Multimedia Revolution.

Now people use computers in all facets of their lives. Computers are used to design graphics, produce full motion video projects, compose music, create and revise business documents, transmit business information through e-mail, make airline or hotel reservations and even participate in online chat rooms for business or pleasure. These activities are made possible by the computer and the transmission of digital information through the Internet.

[A] Discovery Changes

The discovery of evidence has undergone a profound change. One author noted:

> The courtroom is the crucible of the law, where the fire of litigation tests the intellectual and political forces that inform social policy. Discovery - the process by which litigants identify and assemble their evidence - provides the fuel for the fire. Indeed, not long ago most of the evidence that the discovery process produced was, quite literally, flammable: boxes upon boxes of paper documents. No longer is this the case. Computer technology has taken us from a world of paper to a world of digital media. It has changed almost everything about our relationship with information: how we create it, how much of it we create, how it is stored, who sees it, how and when we dispose of it.

James Gibson, *A Topic Both Timely and Timeless*, 10 Rich. J.L. & Tech. 49 (2004), at http://law.richmond.edu/jolt/v10i5/article49.pdf.

Prior to the 1990s, most cases involved the discovery of paper documents. It was, and still is to a large extent, the norm to obtain printed discovery material and then copy and recopy, categorize, Bates number and then file them in three-ring binders or expandos. However, it is estimated that more than 30 percent of corporate communications never appear in printed form and more than 97 percent of information is created electronically. Peter V. Lacouture, *Discovery and Use of Computer-Based Information in Litigation,* 45 R.I.B.J. (1996); John H. Jessen, *Special Issues Involving Electronic Discovery,* 9 Kan. J. L. & Pub. Pol'y 425, 442 (2000).

Now it is required to discover not only printed materials, but also electronic information that has not been reduced to hardcopy. In addition to searching for paper documents in corporate archives, file cabinets, branch offices and other physical locations, we are now seeking information contained on hard drives, removable storage media, cell phones and other electronic storage devices.

Discovery materials should be obtained in an electronic format in order to discover metadata that is contained in these materials. Metadata is electronic information that is hidden in an electronic file and may contain valuable data relevant to your case.

Besides the advantage of locating metadata, receiving discovery materials in electronic format will assist you later in searching for specific information using standard litigation support software. Using full text search and retrieval software and/or a database, one can search and retrieve information about a particular person or issue in thousands of e-mail or other electronic information in seconds.

There have been several high profile stories - such as the Microsoft antitrust lawsuit, Monica Lewinsky and Oliver North's "deleted" e-mail - that point out the immense value of electronic information. Even though much publicity has been given to discovering the "smoking gun" from the opposing party, your client's electronic information can also support their claims or defenses. Your client's e-mail, office memos and other communications can often support the factual basis of their case

The process of discovering, producing and presenting electronic information is different and will initially be more difficult than handling paper documents. Instead of worrying about how many copies of a document will be made, you will be focusing on the volume of electronic information, the file format in which you wish to either receive or disclose information, processing and searching software and, ultimately, its presentation in the courtroom. As the electronic discovery process matures, the methodology of discovering and producing electronic information will become commonplace. The paper discovery model served as a basis during the analog

era. Now that computers are pervasive, the electronic model will serve as the foundation during the digital era.

For most attorneys, their practice of law has not changed nor kept pace with computer technology and discovery rules. They still discover paper documents, even though most documents today are neither typed nor handwritten, and a significant percentage of communications, such as e-mail, are never printed out. This will change. The fact-finding process is beginning to focus on uncovering electronic messaging systems, Internet usage, word processing revisions, metadata and other electronic information relevant to your case. This electronic information discovery process is a critical change and requires attorneys to understand and educate themselves about electronic discovery in order to incorporate it into their normal case preparation process.

§ 1.02 UNIQUE CHARACTERISTICS

Digitized information takes on very different characteristics. As set out below electronic information is different, handled differently and in many ways contains information of greater value than paper information. Always remember that electronic information is not just text or data, but also includes audio, video and graphics.

[A] Informal Nature

Because of its informal nature, electronic mail has encouraged senders to write unguarded, unwise and often inappropriate comments. Though they would never say these things to a person directly or make these written comments in a letter, they will use e-mail to write admissions that are subsequently used in litigation. Part of the reason for this informality is that "[y]ou've got more people who are lower down the chain of command putting things in writing than you did when it was a system of official memos. People are less discreet when they're doing emails." Phil Harris, *Electronic Discovery,* Of Counsel (April 2001). Recognizing that people often make these unguarded remarks, e-mail comments made by the parties and witnesses are more apt to lead to fruitful discovery.

This informal nature of comments also applies to word processing documents that have been revised by one or many authors. Within each word processing file there is what is commonly called metadata that stores the previous revisions and comments. The metadata can be opened and reviewed for unguarded comments by the authors of the documents.

DISCOVERY IN THE DIGITAL AGE

By Mollie Nichols
Senior Vice President and Counsel
First Advantage
mnichols@fadv.com
(703) 374-4346

Discovery in the Digital Age

Table of Contents

Definitions and Background Information

ELECTRONIC DISCOVERY: The production of original evidence in electronic form; such evidence is computer-generated and may exist on, among other locations, hard drives, backup tapes, personal digital assistants, shared (network) storage, CDs, Zip drives, Jaz drives, and floppy disks.

ELECTRONIC DOCUMENTS: Information created, stored, and/or utilized using computer technology, business applications, Internet applications (such as e-mail), peripheral and mobile devices, and computer-based record storage.

ACTIVE DATA: Information that resides on the user's hard drive and/or network server and is readily available and accessible to computer users through file manager programs.

BACKUP DATA: Information copied to a removable media, such as a tape, for the purpose of disaster recovery, such as a system failure; usually contains everything on a server or some other centralized storage medium or network; often in a compressed form.

FILE SLACK: partial data from an older file or files still residing on the hard drive that has been allocated to a newer file but not used up by this newer file.

FREE SPACE: space on hard drive (or other storage medium) that appears to contain no data because this space is unused or because data that had been intact and accessible at one time are now erased.

LEGACY DATA (Archival Data): Information stored on media that is not in a user-friendly format and difficult to access; can no longer be accepted or organized in a format that can be read using current software; may have to hire technician to write program to retrieve data.

METADATA (or Embedded Data): Data about data, consisting of information within the electronic version of a document that travels with the file and that may not be apparent in a printed version of the document or when viewed on the monitor, such as author, title, subject, size of file, editing history, distribution route of document.

MIRROR IMAGE (Bit Stream Image): Process of creating an exact duplicate of computer memory onto secure storage medium; includes all files, file slack, errors, and residual space.

RESIDUAL DATA: Deleted files and e-mail to which the reference has been removed from the directory listings and file allocation table, and therefore, may be overwritten with another file; usually recoverable until overwritten.

Basic Rules For Computer Forensics:

1. Do not alter original evidence.
2. Do not execute programs on a computer that contains discoverable electronic data (especially programs affecting the operating system).
3. Do not allow anyone who is not properly trained or authorized to interact with the computer; in other words, isolate and preserve the computer.
4. Always create a mirror image of a computer hard drive using the proper forensic tools and work with the mirror image; never alter the original.
5. Document all investigative activities.

Four Points to Remember About Electronic Discovery:

1. Electronic documents are NOT the same as printed documents.
2. Attorneys have a duty to preserve potentially relevant evidence (including evidence in electronic form) when they reasonably anticipate litigation.
3. Attorney must deal with electronic data as soon as possible because this information can easily disappear.
4. Since discovery rulings are interlocutory, appeals on discovery rulings are unusual. Appellate law on electronic discovery is undeveloped. Most decisions are trial-level decisions, and on some points these decisions vary widely.

Why is Electronic Discovery an Issue?

1. Information exists primarily in digital form. Think about your own computer use or your firm's computer use. There are various estimates about the increased use of computers to generate electronic documents. Millions of transactions with legal significance are generated using computer technology.
2. Statistics on the increase in digital information.
    a. A 2003 study at UC Berkeley Study entitled, *How Much Information* estimates that 93% of all information generated in 1999 was in digital form and 70% never migrated to paper.
    b. International Data Corporation found that 31 billion emails were sent each day in 2003. By 2006, 60 billion emails will be sent each day.
    c. In *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 429 (S.D.N.Y. 2002), the court cited authority that one-third of all electronic documents as never printed.

Evolving Legal Duties

1. General Overview of Legal Duties and Obligations

    a. The rules have not changed regarding preservation and production of relevant evidence. The nature and volume of the evidence, however, are different. Electronic evidence can easily disappear, be altered or destroyed if not properly preserved.

    b. FED. R. CIV. PRO. 26(a)(1)(B) provides for mandatory disclosure of electronically stored information that the disclosing party may use to support its claims or defenses. Counsel, not administrative support personnel, will have to make important decisions about case strategy at an early stage in the litigation. (Attachment 1)

    c. To take any ambiguity out of Rule 26(a), amendments, effective December 1, 2006, require that parties provide "a copy of, or a description by category and location of,… electronically stored information,…" without waiting for a discovery request. Amended FED. R. CIV. PRO. 26(a).

    c. The obligation to search for electronic documents arises with FED. R. CIV. PRO. 34(a). *McPeek v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001). Amended FED. R. CIV. PRO. 34(a), effective December 1, 2006, specifically allows parties to request production of and to "test or sample any designated… electronically stored information (including…sound recordings, images, … and other data or data compilations stored in any medium"…)

2. Take the Defensive: The Duty to Preserve

    a. When to preserve electronic documents

        i. Case law determining the point at which the duty to preserve commences varies by jurisdiction, but the most common statement on this duty is that the obligation to preserve evidence that may be relevant begins when the party has notice that potential litigation is likely or that it reasonably anticipates litigation. *Zubulake v. UBS Warburg*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003); *Renda Marine, Inc. v. United States*, 58 Fed. Cl. 57, 61 (Fed. Cl. 2003); *Thompson v. General Nutrition Co.*, 593 F.Supp. 1443, 1450 (C.D.Cal. 1984); *see* ABA Civil Discovery Standards at IV, "Document Production," ABA Section of Litigation (August 2004).

        ii. In *Zubulake v. UBS Warburg* ("*Zubulake* I"), 220 F.R.D. 212, 217 (S.D.N.Y. 2003), the court held that the duty to preserve arose when an email labeled attorney-client privilege was sent without an attorney's active or passive participation, even though it was six months prior to the filing of an EEOC notice. In *Turner v. Hudson Transit Lines*, 142 FRD 68 (S.D.N.Y 1991), the court said the duty to preserve could arise *prior to the filing of the complaint* if a party is on notice of pending litigation. In *Lewy v. Remington Arms Co.*, 836 F.2d 1104 (8th Cir. 1988), the court

said there is a duty to preserve where the information is likely to be relevant to foreseeable litigation. In *Trevino v. Ortega*, 969 S.W.2d 950 (Tex. 1998), the court agreed, stating " a party should not be able to subvert the discovery process and the fair administration of justice simply by destroying evidence before a claim is actually filed… in spoliation cases a party should be found to be on notice of potential litigation when, after viewing the totality of the circumstances, the party either actually anticipated litigation or a reasonable person in the party's position would have anticipated litigation."

iii. The receipt of a complaint may trigger the duty, *NOW v. Cuomo*, 1998 WL 395320 (S.D.N.Y. July 14, 1998), but certainly the receipt of a discovery request does.

iv. In our view, a good guideline before the lawsuit is actually filed and served is that the duty to preserve arises where counsel believes the attorney-work product privilege attaches, that is when the attorney reasonably anticipates litigation. It may be difficult to assert the work product privilege if you are not taking steps to preserve digital data.

v. We have provided suggested steps for counsel to take at the earliest possible time (Attachment 2). Counsel should take a systematic approach to electronic discovery because the volume of electronic data can be overwhelming. In *Danis v. USN Communications, Inc*., 2000 U.S.Dist. LEXIS 16900 (N.D.Ill. Oct. 20, 2000), the court details how complex and mistake-ridden massive electronic document production can be. Both parties made representations to the court and allegations against each other's compliance with the discovery obligations that showed neither party understood what information each already had in its possession.

b. What must be preserved

i. Active files vs. residual data in free space or slack space. We have explained the differences, but refer to the definitions. Active files must be preserved.

ii. There is some argument whether residual files, i.e., data that has been "deleted," are in the party's possession or they are the equivalent of documents already shredded or discarded in the dumpster.

1. Many courts have held that deleted data is discoverable. In *Kleiner v. Burns*, 2000 WL 1909470, at *4 (D. Kan. Dec. 15, 2000), the court noted that computerized data includes deleted email and is discoverable. *See also Simon Property Group v. mySimon, Inc*., 194 F.R.D. 639 (S.D. Ind. 2000), citing *Crown Life Insurance Co. v. Craig*, 995 F.2d 1376 (7th Cir. 1993)("First, computer records, including records that have been deleted, are documents discoverable under FRCP 34."); *Antioch Co. v. Scrapbook Borders, Inc*., 210 F.R.D. 645, 652 (D. Minn. 2002)("It is a well accepted proposition that deleted computer files, whether they are emails or otherwise, are discoverable."); *Zubulake v. UBS Warburg*, 217 F.R.D. 309, 317 (S.D.N.Y 2003) (discovery is permissible of "electronic documents that are currently is use, but also of documents that may have been deleted…"); *Zhu v. Pittsburgh State University*, 2003 US Dist LEXIS 6398 (D. Kansas Feb. 5, 2003), (where the plaintiff moved to compel his former employer to produce computer generated documents reflecting the salaries of other faculty working within his department. Defendant argued that it produced all paper documents that existed and this was sufficient. The court agreed with plaintiff and found that Rule 34 applied to electronic data compilations from which information could have been obtained only with the use of "detection devices." The court required defendants to take reasonable steps to ensure that it disclosed back-up copies of files and archival tapes that will provide information about any "deleted" electronic data.)

2. However, in *Rowe Entertainment, Inc. v. William Morris Agency, Inc*., 205 F.R.D. 421, 429 (S.D.N.Y. 2002), in discussing whether a defendant would be compelled to retrieve deleted e-mail messages, the court noted that plaintiff had made no showing that this defendant accessed its backup tapes or deleted e-mails in the normal course of its business. In these circumstances, the court analogized deleted e-mail messages to hard copy documents that had been discarded in the trash, which a defendant would not be compelled to resurrect. The court declined to compel defendant to retrieve deleted e-mail messages.

3. Even if residual data may not be required to be produced in every case, this type of electronic data is discoverable with a showing of deceptive conduct during discovery. In *Illinois Tool Works, Inc. v. Metro Mark Products, Ltd*., 43 F.Supp. 2d 951 (N.D. Ill. 1999), a critical computer suddenly stopped functioning a few days after the entry of a court order to preserve the integrity of all computers in defendant's possession. Deleted documents were recovered.

4. A party's admission that e-mail messages had been routinely deleted in the ordinary course of business after the lawsuit was filed was part of the basis for the court to permit Playboy to access the computer hard drive to attempt to recover the deleted e-mail messages. *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp. 2d 1050 (S.D. Ca. 1999).

GENERAL RULE: if you think relevant evidence resides in free space or slack space, its best to preserve it. Given the pervasive nature of electronic documents and the fact that a "deleted" document is probably recoverable, we believe you should be prepared to produce residual files.

c. Sanctions

i. Sanctions have been imposed for failing to preserve electronic evidence. The Court of Appeals of California, Fourth District found that a defendant's destruction of payroll records was sanctionable spoliation even though the information was still available in paper form. The court found that the computer documents were more easily accessible and that plaintiff could not manually extract all the necessary information from the hard copies. It affirmed the trial court's sanctions, which included attorney fees, costs, and $100,000 partial reconstruction. *Lombardo v. Broadway Stores, Inc*., 2002 WL 86810 (Cal. Ct. App. Jan. 22, 2002).

ii. A finding of gross negligence may not be necessary to be the recipient of sanctions. In September 2002, the Second Circuit found a lower court used the wrong legal standard in denying a corporation's motion for an adverse inference instruction when the opposing party failed to produce emails. The Second Circuit found the judge erred in requiring a showing of bad faith or gross negligence as opposed to ordinary negligence; "The sanction of an adverse inference may be appropriate in some cases involving the negligent destruction of evidence because each party should bear the risk of its own negligence." *Residential Funding Corp. v. DeGeorge Fin Corp*, 306 F.3d 99 (2d. Cir. 2002).

iii. At least one court has set forth what a party must do, at a minimum, to properly discharge its discovery obligations. In *Metropolitan Opera Ass'n v. Local 100*, 212 F.R.D. 178 (S.D.N.Y. 2003), the court granted plaintiff's motion for sanctions based upon the failure of defendant and defendant's attorneys to search for relevant paper and electronic documents in response to discovery requests. The court found defendant failed to meet its duty to "establish a coherent and effective system" to respond to discovery requests. The court found that such a system must include (1) a reasonable procedure to distribute discovery requests to those potentially possessing responsive information and a method to account for its collection; (2) a way to explain the types of relevant and responsive information to the client; (3) a systematic process for document collection and retention, including an inquiry into the client's document retention systems; and (4) the supervision of all discovery tasks carried out by non-legal personnel.

iv. An Ohio appeals court has held that the party requesting sanctions must show it was prejudiced by the destruction. In *Hildreth Mfg. v. Semco*, 785 N.E.2d 774 (Ohio Ct. App. 2003), the appellate court upheld the trial court's refusal to grant Semco's motion for contempt after Hildreth destroyed data because there was no indication that the drives contained evidence favorable to Semco.

v. Sanctions include cost shifting, fees, adverse inference instructions, and default judgment:

1. Attorney's fees and costs: *Green v. Baca*, 225 F.R.D. 613 (C.D. Cal. 2005)(attorneys fees of $54,375 ordered as fine); *Nartron Corp. v. General Motors Corp*., 2005 WL 26991 (Mich. Ct. App. Jan. 6, 2005) **(**affirmation of trial court's order requiring plaintiff to pay attorney's fees, costs and interest of over $4 million for intentional alteration of a database); *Trigon Insurance Co. v. United States*, 204 F.R.D. 277, 2001 (E.D.Va. 2001) (government was ordered to pay Trigon's attorneys' fees and costs.); *GTFM, Inc. v. Wal-Mart*, 2000 U.S. Dist. LEXIS 3804 (S.D.N.Y. Mar. 28, 2000); *Illinois Tool Works, Inc. v. Metro Mark Products, Ltd.*, 43 F.Supp.2d 951 (N.D.Ill. 1999).

2. Fines: In *United States v. Philip Morris*, 327 F.Supp.2d 21 (D.D.C. 2004), Philip Morris was ordered to pay $2.75 million in sanctions for destroying e-mails sought by the Justice Department. The sanction was justified based upon the company's "reckless disregard and gross indifference" to a court order requiring preservation of relevant evidence. The company was further prohibited from using testimony at trial of any of the 11 top executives who allowed deletion of the e-mails. In *Danis v. USN Communications*, 53 Fed.R.Serv.3d 828 (N.D. Ill. 2000), the CEO was personally fined $10,000 for delegating preservation responsibilities to an inexperienced attorney who failed to establish a meaningful document retention program noting that there was no general notice to employees to preserve documents, no specific criteria regarding what should be saved, no attorney review of documents being destroyed, and no review of pre-existing practices relating to document preservation, including email, for terminated employees.

3. Adverse Inference Instruction: *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co*., 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005) (After the court found that Morgan Stanley wrongly continued its practice of overwriting emails after 12 months in violation of SEC regulations that require preservation for two years, it required Morgan Stanley to search for and produce the missing emails on back up tapes. Morgan Stanley failed to meet the deadlines imposed by the court, but gave a false certification of full compliance with the court's order. At the time the false certification was made, over 2000 back-up tapes had not been processed. Morgan Stanley attempted to produce the data by using in-house IT staff, but lacked the technological capacity to upload and search the data requested and missed email attachments and 7,000 Lotus Notes emails due to flawed software scripts written by Morgan Stanley. On March 1, 2005, the court granted plaintiff's motion for an adverse inference instruction based on Morgan Stanley's destruction of email and a variety of other eDiscovery abuses); *Zubulake v. UBS Warburg, "Zubulake IV"*, 220 F.R.D. 212 (S.D.N.Y. 2003) (because an adverse inference instruction is a severe sanction

that "often ends litigation," the party must show a duty to preserve, destruction with a "culpable state of mind" and that the destroyed evidence was relevant to the requesting party's claim or defense.) *See also Shamis v. Ambassador Factors Corp.*, 34 F.Supp.2d 879 (S.D.N.Y. 1999); *Linnen v. A.H. Robins Co.*, 10 Mass. L. Rptr. 189 (Super. Ct. 1999); *Reingold v. Wet N' Wild Nevada, Inc*., 944 P.2d 800 (Nev. 1997); *Shaefer v. RWP Group, Inc*., 169 F.R.D. 19 (E.D.N.Y. 1996).

4. Default Judgment or Dismissal: *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co.*, 2005 LEXIS 94 (Fla. Cir. Ct. March 23, 2005.) The Court in *Morgan Stanley* granted a partial default judgment against Morgan Stanley after defendant "deliberately and contumaciously violated numerous discovery orders," including "hid[ing] information about its violations and coach[ing] witnesses to avoid any mention of additional, undisclosed problems with its compliance" with the court's orders. At trial, the court read a statement to the jury about Morgan Stanley's discovery practices, and told the jury "that it may consider those facts in determining whether [Morgan Stanley] sought to conceal its offensive conduct when determining whether an award of punitive damages is appropriate." The jury returned a verdict against Morgan Stanley of $1.45 billion.; *Nartron Corp. v. GMC*, 2003 WL 1985261 (Mich. Ct. App. Apr. 29, 2003) (affirmation of dismissal of plaintiff's case after court found several discovery abuses occurred, including fabrication and destruction of computer records); *Kucala Enterprises v. Auto Wax Co*., 56 Fed. R. Serv. 3d 487, *adopted as modified*, 56 Fed. R. Serv. 3d 487 (N.D. Ill 2003) (Court dismissed case after a computer wiping program "Evidence Eliminator" was used to destroy evidence on a laptop after the court had entered a preservation order and hours before the opposing parties' computer forensic expert was to examine the computer.); *See also Commissioner of Labor of North Carolina v. Ward*, 580 S.E.2d 432 (N.C. App. 2003); *Essex Group v. Express Wire Services*, 578 S.E.2d 705 (N.C. Ct. App. 2003).

5. Other: *In the Matter of Rebecca Arlene Ware*, 112 P.3d 155 (Kan. 2005)(disciplinary hearing where attorney suspended for one year after she did not defend company in employment litigation and deleted a case tracking log from computer; *DirectTV, Inc. v. Borow*, 2005 WL 43261(N.D. Ill. Jan 6, 2005)(after defendant ran "Evidence Eliminator" to erase data after filing of complaint, summary judgment granted for plaintiff.)

vi. *See Trevino v. Ortega*, 969 SW2d 950 (Tex. 1998), for a lengthy discussion on spoliation-related sanctions under Texas law.

vii. Many businesses have established record management programs. These programs create special problems for potential spoliation claims. An ABA survey conducted in May 2000 asked attorneys involved in litigation whether their clients had an established protocol for handling electronic discovery requests, and 83% said no.

Due to the nature of electronic documents, record management and/or disaster recovery policies represent a significant concern for counsel. We recommend counsel determine at the earliest time whether the client has one or both of these programs. (*See* Attachment 2). The best practice is to work with clients before litigation arises to prepare a protocol to suspend the policy, known as a litigation hold, when the duty to preserve information arises.

1. In *Lewy v. Remington Arms Co.*, 836 F.2d 1104 (8th Cir. 1988), the court established a standard to determine the reasonableness of a record management program. Remington had destroyed certain documents pursuant to its 12-year old corporate record retention program. The trial court had instructed the jury that they could draw a negative inference from Remington's inability to produce the records. The 8th Circuit remanded for further consideration of the reasonableness of the record retention policy under four criteria: (a) whether the policy is reasonable considering the facts and circumstances regarding the relevant documents; (b) whether certain documents are relevant in litigation and how frequently such litigation is filed; (c) whether the policy was adopted in bad faith; and (d) whether under the circumstances documents should be retained despite the policy (e.g. when the corporation knows or should know that the documents will be material in the future). The Court said a corporation may not blindly destroy documents pursuant to a stated policy and expect to be shielded from liability in all circumstances.

2. Record retention policies are created to reduce the potential liability for spoliation, but they can create a risk of spoliation if they are improperly drafted or used improperly. In *Trigon Insurance Co. v. United States*, 204 F.R.D. 277 (E.D.Va. 2001), key testimonial experts of a firm hired by the government had deleted many drafts of their reports and communications with each other in accordance with the document retention policy of their firm. This destruction caused the firm to have to pay computer forensic experts to restore as much of the deleted documents as they could and ultimately cause the government to have to pay Trigon's attorneys' fees and costs in connection with the spoliation issue.

3. Other courts have raised similar concerns about record retention policies. *See, e.g., Carlucci v. Piper Aircraft Corp*., 102 F.R.D. 472 (S.D. Fla. 1984) (a bona fide, consistent and reasonable document retention policy may be a valid justification for failure

to produce documents – but the court entered a default judgment against Piper for its inadequate administration).

4. An improper, unreasonable or unenforceable document retention policy may be just as harmful as no policy at all. *See, e.g., In re Prudential Ins. Co. of America Sales Practices Litigation*, 169 F.R.D. 598 (D.N.J. 1997) (Prudential's haphazard and uncoordinated approach to document retention indisputably denied its opponents potential evidence to establish facts in dispute and was grounds for severe sanctions – a fine of $1 million imposed on Prudential).

5. In *Stevenson v. Union Pacific R. Co*., 354 F.3d 739 (8th Cir. 2004), the Court of Appeals reviewed the trial court's partial summary judgment and adverse-inference instruction against the defendant as a sanction for destroying recorded voice radio communications between the train crew and dispatchers pre-litigation, as well as track maintenance records both pre- and post-litigation.. The instruction was given as sanction for destroying the audiotapes because they were clearly relevant to reasonably anticipated litigation, there were no alternative records, and there was evidence that similar recordings had been preserved in other litigation. The court also held that the routine destruction of track maintenance records prior to the filing of the lawsuit and pursuit to a record retention policy did not give rise to a presumption of bad faith.

6. In *Applied Telematics, Inc. v. Sprint Communications Co.*, 1996 U.S. Dist. LEXIS 14053 (E.D.Pa. Sept. 17, 1996), the court concluded that Sprint's normal backup and recycling of backup tapes should have been suspended during the litigation. In *Bowmar Instrument Co. v. Texas Instruments*, 1977 U.S.Dist. LEXIS 16078 (N.D. Ind., May 2, 1977), the court said that records that were destroyed pursuant to a records management policy may be proof of willfulness. In *Reingold v. Wet N' Wild Nevada, Inc*., 944 P.2d 800 (Nev. 1997), the court said that the destruction of relevant and discoverable records pursuant to a records management policy but before the applicable statute of limitations had run on the events covered in the records destroyed amounted to suppression of evidence, and that an adverse inference instruction should have been given to the jury.

7. Some commentators refer to the new provision in FED. R. CIV. PRO. 37, effective December 1, 2006, as a "safe harbor." The Rule states, "Absent exceptional circumstances, a court may not impose sanctions … on a party for failing to provide electronically stored information lost as a result of the routine, good faith operation of an electronic information system." The Rule 37 committee notes state that parties are still required to: (a) modify or suspend certain routine operations to prevent the loss of information "when a party is under a duty to preserve … because of a pending or reasonably anticipated litigation;" and (b) preserve back-up tapes if data is "likely to be discoverable and not available from reasonably accessible sources."

d. How to preserve electronic evidence

   i. Call your client and make a "reasonable inquiry" about the location of potentially relevant evidence. Be sure to ask the proper individual and to document the instructions given. Include some form of verification of the individual's actual compliance with your advice.

      1. *See GTFM, Inc. v. Wal Mart*, 2000 US Dist LEXIS 3804 (S.D.N.Y. Mar. 28, 2000). Counsel for Wal Mart asked a Wal Mart senior executive about certain computer printouts requested by plaintiffs. The executive said Wal Mart could not retrieve them. One year later, defendant's VP in the MIS group was deposed. He revealed that this information was in fact readily retrievable at the time the earlier request was made. Court granted plaintiff's motion to conduct on-site inspection of computer system and for sanctions.

      2. *Zubulake v. UBS Warburg*, 2004 WL 1620866 (S.D.N.Y. July 20, 2004)("*Zubulake V*"). *Zubulake V* holds that attorney's must take "affirmative steps" to ensure clients preserve evidence once litigation is reasonably anticipated. Instructing clients on preservation is not enough. Attorneys must do things such as directly talk to the "key players," instruct all employees to produce relevant electronic evidence, and identify and secure all relevant backup tapes for a company's computer system.

      3. Counsel should instruct client that client should preserve both hard copy and electronic version of the documents. *Thompson v. General Nutrition Co.*, 593 F.Supp. 1443 (C.D. Cal. 1984).

      4. It is the duty of the company to preserve the records. Sanctions may be imposed even if the particular employee responsible for the records in question did not know to preserve the records. *National Association of Radiation Survivors v. Turnage*, 115 F.R.D. 543 (N.D.Cal. 1987).

   ii. *See* Attachment 2 for sample matters to review with client.

   iii. Mirror imaging is only way to preserve residual data. *See, e.g., Gates Rubber Co. v. Bando Chem. Indus. Ltd.*, 167 FRD 90 (D. Colo. 1996). Gates was ordered to preserve computer records, but chose an unqualified computer technician, not a computer forensic expert, to copy the files. The procedure used by Gates' expert overwrote about 8% of the hard drive before he even began to copy the documents. Court concluded that Gates should first have created a mirror image of the hard

drive and thereby captured every piece of information on the hard drive whether the information was allocated as a file or not.

e. Why preserving hard copies is not enough

i. FED. R. CIV. PRO. 26 (a)(1)(B) and FED. R. CIV. PRO. 34 (b) identify data compilations as discoverable documents. The Advisory Notes explicitly state that this includes electronic data from computers. In *McPeek v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001), the court said the obligation to search for electronic documents arises with FED. R. CIV. PRO. 34(a).

ii. It is black letter law that electronic data is discoverable. *Bills v. Kennecott Corp*, 108 F.R.D. 459 (D.Utah 1985); *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 WL 649934 (S.D.N.Y. Nov. 3, 1995); "*Does Discovery of Electronic Information Require Amendment to The Federal Rules of Civil Procedure?"* Commercial & Federal Litigation Section, Committee on Federal Procedure, New York State Bar Assoc. Report (Feb. 22, 2001). With discovery of electronic documents, the issue appears to be how extensive the production of electronic documents must be, not whether electronic documents had to be produced at all. *See Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002).

iii. Taking all ambiguity of the discoverability of data, effective December 1, 2006, the proposed Federal Rules of Civil Procedure refer to "electronically stored information" throughout the new rules. Specifically, FED. R.CIV. PRO. 34 allows parties to request production of and to "test or sample any designated… electronically stored information (including…sound recordings, images, … and other data or data compilations stored in any medium"…)

iv. Metadata is discoverable. In *Williams v. Sprint/United Mgmt. Co.*, 230 F. R. D. 640 (D. Kan. 2005), the court held that when a party is required to produce electronic documents as they are maintained in the ordinary course of business, i.e. native or active files, the documents should be produced with the metadata in tact, unless the party timely objects, the parties agree otherwise, or a protective order is sought.

v. Data is discoverable even if never reduced to printed form. *See, e.g., Crown Life Ins. v. Craig*, 995 F. 2d 1376 (7th Cir. 1993). The court held that computer data is a "document" under the FRCP and must be produced in accessible form. Plaintiff was sanctioned for failing to produce information from a database regarding commissions on each policy defendant sold. The court found the raw data was available to and retrievable by plaintiffs and that plaintiffs had used this data to prepare its own witness and planned to use the data to rebut defendant's case. The court entered default judgment for defendant on his counterclaim.

vi. The requesting party can obtain the data in computerized form even though it possesses the hard copy of the information. *Williams v. E.I. duPont Nemours & Co*., 119 F.R.D. 648 (W.D. Kent. 1987). "[T]he rule is clear; production of information in 'hard copy' documentary form does not preclude a party from receiving that same information in computerized/electronic form." *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 WL 649934 (S.D.N.Y. Nov. 3, 1995); *Rowe Entertainment, Inc. v. Williams Morris Agency, Inc.* 205 F.R.D. 421 (S.D.N.Y. 2002); *Daewoo Electronics Co., Ltd. v. United States*, 650 F.Supp. 1003, 10 C.I.T. 754 (Ct. Int'l Trade 1986); *Adams v. Dan River Mills, Inc.*, 54 F.R.D. 222 (W.D. Va. 1972).

vii. It is also black letter law that the electronic files are different than paper documents. *Armstrong v. Executive Office of the President*, 1 F.3d 1274 (D.D.C. 1993)(printing hard copy of e-mail was not the same as preserving the electronic version. Hard copy did not contain directories, distribution list, acknowledgment of receipts, transmittal information.); *Lombardo v. Broadway Stores, Inc*2002 WL 86810 (Cal. Ct. App. Jan. 22, 2002) (destruction of electronic data still sanctionable spoliation even though hard copy available because it had "unique" and "distinct" evidentiary value.)

viii. *See* Attachment 3 for a short list of reasons why electronic documents are different than paper copy.

ix. Producing party may have to provide requesting party with on-site access to producing party's computer systems, to loan software to requesting party, or to download data from tapes to computer disks or to a hard drive. *Sattar v. Motorola, Inc*., 138 F.3d 1164 (7th Cir. 1998).

x. BOTTOM LINE – relying solely on information in paper form will mean that you are missing important information. There is no reason for not obtaining the information in electronic form. Electronic discovery "could make or break a case." Withers, *Electronic Discovery: The Challenges and Opportunities of Electronic Evidence*, Nat'l Workshop for Magistrate Judges, July 23-25, 2001.

3. Take the Offensive: Ensure Your Opponent is Preserving Data

a. Send preservation letter immediately.

i. A preservation letter will preserve evidence and will give you a basis to seek remedies if opponent fails to comply. In *Wiginton v. Ellis*, 2003 WL 22439865 (N.D. Ill. Oct. 27, 2003), the defendant continued its normal document retention and destruction program for months after receiving a preservation letter from plaintiff explicitly stating that electronic records must be preserved. The Court found that the defendant acted in bad faith, but did not issue sanctions. The Court ordered preservation of the records, and stated that the motion for sanctions could be reconsidered after review by plaintiff's expert of the back up tapes remaining.

ii. Attachment 4 is a sample preservation letter.

b. Other discovery techniques: depositions, interrogatories, and motions

i. At an early stage in discovery, conduct a deposition under FED. R.CIV. PRO. 30b(6) of a representative designated by the corporation. A computer technician may be required to answer questions regarding data storage. A deposition of the opponent's IT representative may be appropriate before proceeding with discovery. These depositions should seek to identify how the opponent maintains its data and what hardware and software are necessary to access the information that may be covered under a Rule 34 Request for Production of Documents. Sample Questions for a Rule 30(b)(6) Deposition are provided in Attachment 5.

ii. In *Carbon Dioxide Industry Antitrust Litigation*, 155 F.R.D. 209, 214 (M.D. Fla. 1993), plaintiffs served a Rule 30(b)(6) deposition notices on defendants. The notices asked each defendant to identify data maintained on its computers as well as the hardware and software necessary to access the information. Even though the court previously had approved a discovery/deposition order, the court ordered the 30(b)(6) depositions to be held because they were necessary to proceed with the merits discovery.

In *Alexander v. FBI*, 188 F.R.D. 111(D.D.C. 1998), plaintiffs filed a Rule 30(b)(6) deposition notice on the Executive Office of the President for information about the system of files, e-mail systems, systems for recording devices, and White House Office databases. The government objected claiming that, in reality, the deposition sought to inquire into the thoroughness of the searches the government had previously completed. The court ruled that the government's affidavit as to the thoroughness of its searches had not been rebutted, and therefore, plaintiffs' notice to inquire on this matter was not supported. The court permitted, however, a Rule 30(b)(6) deposition to proceed to (a) learn about the e-mail systems and the construction of user identification tables; (b) learn about the computer system containing a database of persons who had contacted the White House; and (c) learn about the system for acquisition, location, and disposition of computers.

iii. Preservation Orders from the Court. During the Rule 16(a) conference with the Court, counsel should request a preservation order from the Court. Failure to preserve after the issuance of a preservation order was an issue in *Keir v. UnumProvident Corp.*, 2003 WL 21997747 (S.D.N.Y. Aug. 22, 2003). In June 2003, plaintiff advised the court that electronic records that had been ordered preserved had been erased. The court determined that there were several shortcomings in defendant's efforts to ensure preservation of the materials in question. Because the extent of loss of degree of prejudice to plaintiff could not be determined, the court recommended appointment of an independent expert.

iv. Sample Interrogatories are provided in Attachment 6. Based on the responses, you may decide to seek a protective order, motion to compel, or sanctions. A sample motion to access the hard drive of a computer is provided in Attachment 7. Case authorities for this motion are included.

c. Hire a computer forensics expert

i. A sample engagement letter is provided in Attachment 8.

ii. Several courts have recognized that permitting the computer forensic expert of one party to have unsupervised access to the hard drive of the opponent creates the risk of waiver of the attorney-client privilege, disclosure of trade secrets, and access to irrelevant information. To manage this concern, these courts have followed the protocol first developed in *Playboy Enterprises, Inc. v. Welles*, 60 F.Supp.2d 1050 (S.D.Cal. 1999); followed in *Simon Property Group v. mySimon, Inc.*, 194 F.RD. 639 (S.D.Ind. 2000); *Northwest Airlines, Inc v. Local 2000, Int'l Brotherhood of Teamsters*, C.A. No. 00-08 (D.Minn. February 2, 2000); *See also, The Antioch Co. v. Scrapbook Borders, Inc., et al.*, 210 F.R.D. 645 (Minn. 2002).

iii. The *Playboy* "protocol" includes: court-appointed neutral expert; mirror image of hard drive; expert to recover deleted files and perform searches; potentially responsive files to be turned over initially to counsel for producing party; after review by counsel, relevant and non-privileged files are to be produced to counsel for requesting party; requesting party pays for the neutral expert.

iv. In *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 429 (S.D.N.Y. 2002), the court considered adopting the *Playboy* protocol, but chose another protocol. The principal difference from the *Playboy* protocol involves the process of review of potentially privileged e-mail messages of defendants. If defense counsel wanted to conduct the privilege review of the electronic documents prior to their production to plaintiffs' counsel, then defendants would bear the cost of that portion of the production. Otherwise, at plaintiffs' expense, plaintiffs' expert would image hard drives and restore back up tapes; plaintiffs would determine search terms (defendants were allowed to object to the terms); plaintiffs' counsel (not the clients) would receive all documents, whether privileged or not; they would select the responsive documents; they would deliver to defense counsel hard copies of these documents; and defense counsel would object and assert privilege on the appropriate documents. The court decreed that defendants would not be waiving any privilege claim by agreeing to this protocol.

4. Controlling Costs

a. General principles

i. Counsel has the opportunity to manage the scope of discovery under the Federal Rules. Upon motion of counsel or upon the courts own initiative, FED. R. CIV. PRO. 26 (b)(2) (i)-(iii) can be used to limit unreasonable discovery requests.

ii. Given the increasing use of electronic communications and the creation of electronic documents, however, it is unwise to agree that neither side will seek discovery of the other side's electronic files.

iii. While appearing to save money, relying on a client's in-house IT personnel to perform e-discovery functions is unwise because of independence issues, skills factor, lack of knowledge of legal requirements, etc. IT personnel are trained to provide services, not to conduct computer forensics or electronic data recovery. IT personnel are familiar with how computers and computer systems work. Electronic discovery experts are skilled in providing an automated process for discovery of electronic documents. Computer forensic experts specialize in recovering deleted files and restoring legacy data.

b. Cost shifting

i. The responding party's traditional cost-shifting practice of making the documents available for inspection under FED. R. CIV. PRO. 26 and 34 may not be an option with electronic data. There are many reasons for this, such as risking trade secrets, relevancy of much of the data, and complexity of computer systems. The responding party has little choice other than to produce the documentation. In federal court, the presumption is that the producing party bears the cost of producing responsive documents during the discovery process, unless it shows an "undue" burden. *Bills v. Kennecott Corp.*, 108 F.R.D. 459 (D.Utah 1985). (For examples of "undue" burden arguments that were unpersuasive to the court, read *Rowe Entertainment, Inc. v. William Morris Agency, Inc*., 205 F.R.D. 421, 429 (S.D.N.Y. 2002). In *Rowe*, the court was assisted by affidavits from electronic recovery firms that had been retained by several of the parties, including plaintiffs.)

ii. The courts have treated the cost issue differently. There is no bright line rule but three approaches have been used:

1. A balancing approach used in *Rowe Entertainment, Inc. v. William Morris Agency, Inc*., 205 F.R.D. 421, 429 (S.D.N.Y. 2002), *modified by Zubulake v. UBS Warburg,* ("*Zubulake I*") 217 F.R.D 309 (S.D.N.Y. 2003). In *Rowe*, the court used a balancing approach to the question of shifting costs. It applied nine factors in reaching its decision: (1) specificity of the discovery request; (2) likelihood of a successful search; (3) availability from other sources; (4) purposes of retention; (5) does producing party benefit from production; (6) total costs involved; (7) ability to control costs; (8) parties' resources; (9) privileged and confidential documents. *See also, Medtronic Sofamor Danek, Inc. v. Sofamor Danek Holding, Inc*., 2003 U.S. Dist LEXIS 8587 (WD Tenn. May 13 2003)(following the *Rowe* analysis and determining requesting party must pay to produce information from backup tapes.)

Rowe was modified by *Zubulake I* when the court found that *Rowe* test was incomplete and erroneously gave equal weight to all of the factors when certain ones should predominate. The court created a new seven-factor test: (1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production, compared to the amount in controversy; (4) the total cost of production, compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issues at stake in the litigation; and (7) the relative benefits to the parties of obtaining the information. The court found the factors must be weighted in descending order of importance.

In *Zubulake v. UBS Warburg,*, 216 F.R.D. 280 (S.D.N.Y. 2003) , *("Zubulake III")*, the court shifted 25% of the restoration costs to plaintiff because she could not show that the material sought contained indispensable evidence.

2. A marginal utility test. In *McPeek v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001), the court adopted a "marginal utility" approach – i.e., the more likely that a backup tape contains information that is relevant to a claim or defense, the fairer it is that the producing party pay. The less likely, the more unjust it would be for the producing party to pay. The court said that if the likelihood of finding something is the only criterion, someone might have to pay a great deal of money to find one e-mail messages. For the court, this would give the requesting party too great a leverage over the defendant.

3. A foreseeable risk approach. Judges who refuse to shift costs most often use this approach. The courts find that the responding party chose the technology that created the expense of production. Even where the retrieval costs were significant, the court refused to shift costs because it was the producing party's computerized record-keeping scheme that created the costs. For example, in *Linnen v. A.H. Robins Co.*, 10 Mass. L. Rptr. 189 (Super. Ct. 1999), the court refused to shift the cost of production to the requesting party because it believed it would be unfair to permit the company to enjoy the benefits of technology but at the same time use the technology to prevent discovery. The court said that the request to produce electronic documents should be treated in the same manner as a request to produce documents from a filing cabinet, and said producing party bears the expense. *Accord, Bills v. Kennecott Corp.*, 108 F.R.D. 459 (D. Utah. 1985); *In Re Brand Name Prescription Drugs Antitrust Litigation*, 1995 US Dist LEXIS 8281 (N.D. Ill. 1995).

**Several courts have rejected the foreseeable risk approach. For example, in *Rowe*, the court rejected the argument that because

the responding party chose the method of electronic storage, it should therefore bear the cost of production. The court did not agree that the necessity for retrieving stored electronic data is an ordinary and foreseeable risk. In this court's opinion, parties retain electronic data because, unlike paper storage, the costs of storage are nil and there is no compelling cost reason to discard such data. Moreover, the court pointed out that data is not stored for retrieval purposes but is simply uploaded in its entirety onto a backup tape for disaster recovery purposes. Retrieval of individual files or documents is not an underlying purpose of such storage. Also, in *McPeek*, the court rejected an all-or-nothing approach that the producing party has to pay for all restoration costs merely because it chose to use computers. The court noted that if that were the case then the requesting party has no disincentive to demand anything less than all tape.

iii. There are some cases where the court shifted the costs. Applying the cost shifting factors set out in *Zubulake I*, Judge Scheindlin, in *Zubulake III*, reviewed the results of a sampling of defendant's backup tapes to determine the relevancy of the data and the cost of tape restoration before shifting the costs of production with the defendants paying 75% and the plaintiff 25%. The Court in *OpenTV v. Liberate Technologies*, 219 F.R.D. 474 (N.D. Cal. 2003), applied the *Zubulake* factors when ordering that the parties split the cost of extracting the source code from the defendant's database in this software patent infringement case.

iv. The amended Rules provide for a two tier production distinguishing accessible v. not reasonably accessible. FED. R. CIV. PRO. 26(b)(2)(B). Specifically, it reads,"[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost." Keep in mind that accessibility is tied to burden or cost. If a motion to compel is filed and "good cause" (balancing costs and potential benefits) is shown by the requesting party, the court may order production of electronically-stored information that is not reasonably accessible and specify any conditions (amount, type, source to be accessed or cost-shifting).

v. Rule 26's comments state that appropriate considerations by the court also include:

(1) the specificity of the request; (2) quantity of information available from other accessible sources; (3) failure to produce relevant material that was formerly accessible; (4) likelihood of finding relevant, responsive information that cannot be obtained from other, more accessible sources; (5) predictions as to the importance and usefulness of further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources.

5. How to Get a Reasonable Price Quote From an Electronic Recovery Firm

   a. General principles

      i. FED. R. CIV. PRO. 26(a)(1)(B) requires attorneys to think about data that may be used to support their claims or defenses. Hourly or fixed price per documents are of little value in determining the ultimate cost of electronic discovery.

   b. Obtaining a usable quote

      i. Electronic data recovery is a professional service, not a commodity or off-the-shelf item; besides technical expertise, it requires creativity, experience, process management, problem solving, and other skills. It is important to retain a knowledgeable expert. *See Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 429 (S.D.N.Y. 2002) where the court had to consider conflicting affidavits of competing experts in electronic document recovery.

      ii. The mandatory disclosure obligation applies only to documents that will support the client's claims or defenses, not to all of the electronic documents the client may be able to produce. Since only counsel will have developed the strategy for proving the claims or defenses at trial, counsel, and usually not the administrative staff, should be involved in the initial discussions with firms such as First Advantage to obtain a more useful quotation of the estimated cost.

   c. The following are some questions you should expect the provider of electronic data recovery services to ask before providing a quotation:

      i. What is the universe of electronically stored information involved? (e.g., the number of servers, workstations, back-up tapes)
      ii. What is the type of storage? (e.g., Windows based, Unix based, DLT, or DAT)
      iii. What is the size of the storage? (e.g., number of gigabytes)
      iv. What is needed from the storage? (e.g., e-mails, documents, database information, slack space, deleted files)
      v. What can be excluded from the scope of the production? (e.g., what dates, what individuals, and/or what directories or folders can be excluded?)
      vi. What format is required for the production? (e.g., paper, native file format, common file format, remote access)
      vii. Will metadata have to be preserved? (If yes, what is counsel's definition of metadata?)
      viii. What is the deadline for completion?
      ix. Where will the storage media be produced – on site or off site?
      x. If on site, will there be any restrictions on the time that the electronic data may be captured? (e.g., the work may be completed only in the evening and/or on the weekends)
      xi. Will counsel require an expert to be involved in the production to provide an affidavit or testimony?

xii. Is counsel concerned about chain of custody, data security, and/or confidentiality issues?

d. Quotations may use a variety of price elements. Once a quotation has been received, counsel should analyze the price elements as follows:

i. If the quote is for an hourly rate, does the quote provide a cap that will not be exceeded without prior authorization from counsel and does the hourly rate only apply to the time spent by the expert and not the processing time?
ii. If the quote is per page, what pages are to be produced? How will pages be counted?
iii. If the quote is per e-mail user, what is included?
iv. If the quote is per file, what constitutes a file and is the price based on the files processed or only on the files produced?

The answers to these questions will help provide a sound basis to select your firm, but other pricing models can and should be used based on the factors listed above. Counsel should seek out a firm that will provide counsel with predictable pricing so that counsel may predict the ultimate cost of the recovery and production from the outset. It may take a little longer and require obtaining some information about the media at issue to obtain such a quote, but in the long run it is worth it because you will receive useable information at a predictable cost.

6. Admissibility and Authenticity Issues

a. General: The point of all the careful attention to electronic document recovery is to have evidence that is authentic and admissible. In other words, how can a lawyer prove that the electronic document came from a particular place and was not altered? The case law is beginning to emerge to assist counsel in ensuring that the electronic evidence is admissible.

b. Trial court's discretion

i. The decision whether to admit evidence is within the discretion of the trial court and will not be disturbed on appeal unless there is an abuse of discretion. *V Cable, Inc. v. Budnick*, 2001 WL 155323 (2d. Cir. Dec. 3, 2001)(unpublished). In *V Cable*, the owner of the company whose computers and computer records were seized in executing a search warrant testified that there were some "discrepancies" in the computer invoices being offered by the government into evidence over the objection of Budnick, but he recognized the records, they had the same layout as his business normally used, they contained his unique abbreviations, they were consistent with the records his firm used in the regular course of its business, and he did not see anything in the records to indicate they were inaccurate.

ii. On the opposite side of the scale is *Harveston v. State*, 798 So.2d 638 (Miss. Ct. App. 2001). Harveston was charged with breaking into cars and stealing the contents. As part of the State's proof, the State called a police officer to establish that Harveston did not own the cars involved. The officer testified, over Harveston's objection, that he verified the ownership of the cars by checking a computer database and submitted a printout of the officer's search. This was error because the State failed to establish the necessary predicate – the reliability of the information in the computer records. This is determined by the competence of the compiler of the information and not by the extent of the user's reliance on the information received from the computer.

c. Emails as evidence

i. Self-authenticating - E-mail messages alleged to have been sent by the defendant may be authenticated by introducing evidence that (1) the e-mail address of the sender matches that of defendant's; (2) the e-mail address was the one used by other witnesses who sent messages to defendant; (3) the use of the reply function by its recipient automatically called up defendant's address; (4) the content of one e-mail showed the author knew specific details of the matter under indictment; (4) the messages were signed with the defendant's nickname; and (5) the defendant spoke with recipients personally and repeated the substance of the e-mail messages. *United States v. Siddiqui*, 235 F.3d 1318, 1322 (11th Cir. 2000).

ii. Business Record, present sense impression, and excited utterance: In *US v. Ferber*, 966 F. Supp. 90 (D. Mass. 1997), the offering party attempted to introduce an email under the business records exception to the hearsay rule. An employee sent an email to his superior recounting a conversation between this employee and the defendant, in which the defendant inculpated himself. To support that the email was a business record, the employee testified that it was his regular course of business to report such activities via email to his superiors. The court refused to admit the email finding insufficient evidence that the employee was required to maintain such records. Next, the government tried to admit the email using the excited utterance exception, by arguing that the employee wrote the email shortly after his conversation with the defendant and the employee felt "upset and panicked" following the conversation. The court refused to admit the email under FED. R. EVID. 803(2) finding that this was not the typical outburst that qualifies as an excited utterance. Finally, the government tried the present sense impression exception by arguing that the email was "a statement describing or explaining an event or condition, or immediately thereafter." FED. R. EVID. 803(1). The court agreed and admitted the email into evidence.

iii. Circumstantial evidence: In *People v. Downin*, 828 N.E. 2d 341 (Ill. App. Ct. 2005), the defendant argued that emails should not be admitted without evidence that linked the emails to his IP address. The court disagreed and held that circumstantial evidence was sufficient to establish authenticity. In this case, the victim testified that the information contained in the emails was only known by her and the defendant.

iv. It may be necessary to challenge that authenticity of an e-mail. This can be done through a computer forensic expert. The forensic expert said that plaintiff took the header from another e-mail sent by one of the defendants, altered the substance of that message to enable him to defeat the Statute of Frauds defense defendants had raised. Based on this opinion, the court dismissed the complaint and ordered plaintiff to reimburse defendants for the expert's fee and the fees and expense incurred by defendants' counsel in connection with discovery. *Munshani v. Signal Lake Venture Fund*, 2001 WL 126954 (Mass.Super. Oct. 9, 2001).

d. chain of custody

i. Civil lawyers are now faced with establishing chain of custody for the admission of evidence, a procedure that had primarily been used in criminal matters. When there is a chance that evidence has been commingled or confused, or an allegation that evidence has been altered, proof of chain of custody is important.

ii. Typically, a chain of custody witness in an electronic discovery case will testify about the origin of the data, collection procedure, and storage and handling of the data by referring to a log sheet that was completed at the time of collection. In order to avoid allegations of alteration, it is recommended that a forensically sound image be taken of the file(s) and a hash value, the number generated when a mathematical algorithm is applied to a computer file, be obtained. This unique number whether associated with a file or an entire disk should be identical to the hash value of the original. In *Taylor v. State*, 93 S.W. 2d 487 (Tex. App. 2002), the court of appeals reversed a conviction (1) when the data from a hard drive was authenticated by an officer who failed to record a hash value in any written form, even though he testified that the hash value of the copy was identical to the original; (2) when the officer copied the defendant's hard drive onto another drive that had not been wiped and was deemed "contaminated" since the child pornography could have been on the drive where the copy was stored; and (3) when the officer executed a format command against the defendant's drive, when he should have formatted the target drive. "By doing so, he destroyed the file allocation table for [the defendant's] computer and there was no structure in place for the files which were copied…" *Id*. at 498-508.

ATTACHMENT 1

Federal Rule of Civil Procedure 26

(a)(1) – Initial Disclosures

. . . a party must, without awaiting a discovery request, provide to other parties:

(A) the name and, if known, the address and telephone number of each individual likely to have discoverable information that the disclosing party may use to support its claims or defenses, unless solely for impeachment, identifying the subjects of the information;

(B) a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment;

* * *

. . . A party must make its initial disclosure based on the information then reasonably available to it and is not excused from making its disclosure because it has not fully completed its investigation of the case or because it challenged the sufficiency of another party's disclosures or because another party has not made its disclosures.

(b)(1) In general . . . For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. All discovery is subject to the limitations imposed by Rule 26(b)(2)(i), (ii), and (iii).

(b)(2) Limitations.

(A) By order, the court may alter the limits in these rules on the number of depositions and interrogatories or the length of depositions under Rule 30. By order or local rule, the court may also limit the number of requests under Rule 36.

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

(C) The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden

or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the proposed discovery in resolving the issues. The court may act upon its own initiative after reasonable notice or pursuant to a motion under Rule 26(c).

Amended Federal Rule of Civil Procedure 26

(effective December 1, 2006)

Rule 26. General Provisions Governing Discovery; Duty of Disclosure

(a) Required Disclosures; Methods to Discover Additional Matter.

(1) Initial Disclosures. Except in categories of proceedings specified in Rule 26(a)(1)(E), or to the extent otherwise stipulated or directed by order, a party must, without awaiting a discovery request, provide to other parties:

(A) the name and, if known, the address and telephone number of each individual likely to have discoverable information that the disclosing party may use to support its claims or defenses, unless solely for impeachment, identifying the subjects of the information;

(B) a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment; * * * * *

(b) Discovery Scope and Limits. Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows:

* * * * *

(2) Limitations.

(A) By order, the court may alter the limits in these rules on the number of depositions and interrogatories or the length of depositions under Rule 30. By order or local rule, the court may also limit the number of requests under Rule 36.

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

(C) The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues. The court may act upon its own initiative after reasonable notice or pursuant to a motion under Rule 26(c).

* * * * *

(5) Claims of Privilege or Protection of Trial Preparation Materials.

(A) Information Withheld. When a party withholds information otherwise discoverable under these rules by FEDERAL RULES OF CIVIL PROCEDURE 55 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.

(B) Information Produced. If information is produced in discovery that is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being FEDERAL RULES OF CIVIL PROCEDURE notified, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved.

* * * * *

(f) Conference of Parties; Planning for Discovery. Except in categories of proceedings exempted from initial disclosure under Rule 26(a)(1)(E) or when otherwise ordered, the parties must, as soon as practicable and in any event at least 21 days before a scheduling conference is held or a scheduling order is due under Rule 16(b), confer to consider the nature and basis of their claims and defenses and the possibilities for a prompt settlement or resolution of the case, to make or arrange for the disclosures required by Rule 26(a)(1), to discuss any issues relating to preserving discoverable information, and to develop a proposed discovery plan that indicates the parties' views and proposals concerning:

*** * * * ***

(3) any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced; (4) any issues relating to claims of privilege or protection as trial-preparation material, including – if the parties agree on a procedure to assert such claims after production – whether to ask the court to include their agreement in an order;

ATTACHMENT 2

Suggested Steps for Counsel to Take At Earliest Possible Time

1. Take these steps at least as early as you would claim the protection of the attorney-work product privilege, preferably even earlier.

2. Learn about client's technology.

3. Identify and meet with your client's Rule 30(b)(6) IT representative.
    a. Go over this person's knowledge of client's computer systems, including hardware and major, company-approved software
    b. Go over this person's knowledge of client's networking configurations and accessing of client's computer systems by 3rd parties
    c. Go over this person's knowledge of employees' use while at their residences of computers for business purposes
    d. Learn about the client's disaster recovery backup procedures, including where backup tapes are stored, how long, and legacy systems that may have been used
    e. Advise this person about how backup procedures should be modified to prevent unintended spoliation
    f. Identify a manager of client who has sufficient authority within client's organization to oversee the notification and compliance with preservation of electronic data/compilations until further notice – include verification and compliance with these instructions

4. Identify and meet with your client's Rule 30(b)(6) records management representative.
    a. Go over client's records management policy and ongoing procedures. Determine if this policy addresses electronic documents and placing a "legal hold," which suspends the destruction of documents, including electronic documents, when litigation is probable or underway. Also, find out how the client educates employees about policy compliance; how the policy is audited for compliance; and how the policy is enforced.
    b. Advise this person about suspending portion of record management procedures that entail deleting company records to prevent unintended spoliation.
    c. Identify a manager of client who has sufficient authority within client's organization to oversee the notification and compliance with suspension of any destruction of records pursuant to the client's ongoing records management program until further notice – include verification and compliance with these instructions

5. Review your discovery materials to ensure that the standard instructions and definitions address electronic compilations/data are clear, and up-to-date. Modify these materials as appropriate for the instant litigation.

ATTACHMENT 3

A Few Reasons Why An Electronic Document Is Different From A Paper Document

1. When you used the "delete" key, an electronic document is not discarded. Unlike a paper document that is shredded or burned and unrecoverable, an electronic document may be recoverable.

2. There are far more electronic documents created every day than a paper document, and most of the electronic documents are not intended to be printed.

3. An electronic document contains 'embedded information," usually called metadata. Metadata – data about data – does not appear in the paper version or on the computer monitor. From the original electronic version, a computer forensic expert can determine the original author, date and time of creation, size of a file, how the document was edited and routed, and even various drafts of the electronic document.

4. Electronic documents are more portable and are likely to reside in multiple locations. A person does not need to tote a box of documents but may simply carry a CD or floppy disk. With network systems and the Internet, documents that may be admissible under FED. R. EVID. 1003 as duplicates of an original may be recovered in many locations.

5. Electronic documents may be searched in multiple ways, such as by name, phrase, or date.

6. Multiple copies of an electronic document may be created without the knowledge of the originating author. Replicant data, Network data, Internet Cache, Swap files are examples.

7. Electronic documents, particularly e-mail messages, are often more casually made than paper documents.

8. Electronic documents are often stored and filed in a less organized manner than paper files. Backup tapes are made for purposes of disaster recovery, not for discovery in litigation. IT personnel who create the backup tapes give little thought to organization of data preserved on the tapes themselves.

9. The hardware and software are upgrade and replaced as often every three years. This creates the problem that to access tapes or other storage media on which electronic documents relevant to the dispute have been retained is more complicated and expensive. Hardware that can accept the electronic document and software that can read the document may not be promptly available. This contingency is called the problem of legacy data. Paper documents do not create this problem.

Recovery and analysis of electronic documents will require retaining experts. The process is not the same as searching files for paper documents and photocopying the documents produced.

ATTACHMENT 4

Sample Letter Addressing Preservation of Evidence

Dear _____:

We represent _____ [Plaintiff/Defendant] in this matter.

As you know, Federal Rules of Civil Procedure 26(a)(1)(B) and 34 (a) and applicable case law provide that electronic documents are discoverable. The Federal Rules regarding destruction of evidence apply to electronic data in the same manner as the rules apply to other forms of evidence.

[Plaintiff(s)/Defendant(s)] consider electronic data to be an important and irreplaceable source for discovery and/or evidence. Today, over 90% of all information is generated in electronic form. Millions of transactions with legal significance take place daily using computer and/or electronic technology. We intend to submit discovery requests to access your client's computer network(s) and computer systems and to seek the production of documents in their electronic form. Access to the computer network(s) and computer systems as well as access to documents in their electronic form is critical because the paper form of text derived from an electronic file does not preserve the totality of information that is in the electronic file itself. Therefore, preservation and production of the paper text alone does not constitute the full preservation of evidence.

We request that a copy of this letter be provided promptly to the person(s) who are responsible for your client's computer network and computer systems and to the person(s) who are responsible for your client's record management program. Until the parties reach agreement for the protocols to discover electronic documents and this agreement is memorialized in an order of the court, we request that your client take the broadest view of their obligation under the Federal Rules to preserve relevant electronic documents and take the following steps to safeguard against the destruction of evidence.

Specifically, we request that your client preserve:

a) All electronic mail and information about electronic mail (including message contents, header information and logs of electronic mail system usage) sent or received by [list names, job titles, or job responsibilities];

b) All other electronic mail and information about electronic mail (including message contents, header information and logs of electronic mail system usage) about [describe the subject matter];

c) All data bases (including all records and fields and structural information in such databases) containing any reference to and/or information about [describe the subject matter];

d) All logs of activity on computer systems that may have been used to process or store electronic data containing information about [describe the subject matter];

e) All word processing files and file fragments containing information about [describe the subject matter];

f) All electronic data and file fragments created by application programs which process financial, accounting and billing information about [describe the subject matter];

g) All electronic files and file fragments containing information from electronic calendars and scheduling programs regarding [describe the subject matter];

h) All electronic data files and file fragments created or used by electronic spreadsheet programs where such data files contain information about [describe the subject matter]; and

i) All other electronic data containing information about [describe the subject matter].

To minimize the risk of spoliation of relevant electronic documents, your client also:

Should not modify or delete any electronic data files that are maintained in on-line storage and/or direct access storage devices which exist as of the delivery of this letter and meet the criteria of ¶¶ (a) – (i), unless a true and correct copy of each such electronic data file has been made and steps have been taken to ensure that such copy will be preserved and accessible. (On-line storage and/or Direct Access storage)

Should stop any activity that may result in the loss of such electronic data meeting the criteria of ¶¶ (a) – (i) in electronic media used for off-line storage, including magnetic tapes and cartridges and other media. This activity includes rotation, destruction, overwriting and/or erasure of such media in whole or in part. (Off-line Storage)

Should preserve any electronic data storage devices and/or media that may contain electronic data meeting the criteria of ¶¶ (a) – (i) which may be replaced due to failure and/or upgrade or for any other reason. (Replacement of Data Storage Devices)

Should not alter or erase such electronic data meeting the criteria of ¶¶ 1(a) –(i) and should not perform any other procedures (such as data compression and disk de-fragmentation or optimization routines) which may impact such data on any stand-alone microcomputers and/or network workstations, unless a true and correct copy had been made of such active files and of completely restored versions of such deleted electronic files and file fragments and unless copies have been made of all directory listings (including hidden files) for all directories and subdirectories containing such files, and unless arrangements have been made to preserve copies. (Fixed Drives on Standalone Personal Computers and Network Workstations)

Should preserve copies of all application programs and utilities that may be used to process electronic data described in ¶¶ 1(a) – (i). (Programs and Utilities)

Should maintain an activity log that documents all modifications made to any electronic data processing system that may affect the system's capability to process any electronic data meeting the criteria described in ¶¶ (a) – (i). (Log of System Modifications)

Should to take the following steps immediately with respect to all personal computers used by [list personnel] and/or their secretaries or assistants. (Personal Computers)

- A true and correct copy should be made of all electronic data on fixed drivers attached to such personal computers relating [describe subject matter], including all active files and completely restored versions of all deleted electronic files and file fragments.
- Full directory listings (including hidden files) for all directories and subdirectories (including hidden directories) on such fixed drivers should be written.
- The copies and listings made should be preserved until this matter reaches its final resolution.
- All floppy diskettes, magnetic tapes and cartridges, and other media in connection with such computers prior to the date of delivery of this letter containing any electronic information relating in any manner to the matters in dispute should be collected and put into storage until this matter reaches its final resolution.

Should take whatever steps are appropriate to preserve relevant evidence created subsequent to this letter. (Evidence Created Subsequent to this Letter)

We appreciate your prompt attention to these matters. Please contact me if you have any questions.

ATTACHMENT 5

Sample Rule 30(b)(6) Deposition Questions

Counsel will have his/her own style for framing questions of the Rule 30(b)(6) deponent. Here are some suggested subject areas to address during the Rule 30(b)(6) deposition:

1. Qualifications and Organizational Structure:
   a. Education, training or experience of the deponent [particularly experience or training in handling and investigating computer evidence; IT personnel are trained to provision systems and lack training in forensics].
   b. Where in the organization does the deponent sit – to whom does the deponent report and who reports to the deponent.
   c. The company's use of consultants or outside vendors for maintenance and service of computer systems (hardware, software, and networks).
   d. The role/responsibility the deponent has (or will have) in responding to discovery requests seeking production of electronic documents, such as information created, stored, and/or utilized using computer technology.
   e. Steps taken by deponent to prepare for deposition, including document review.
2. Information about the party's systems:
   a. Duties of system administrators
   b. Use of passwords by users, sharing of passwords, access to passwords by system administrator(s)
   c. Details about hardware used by deponent's employer (may include model numbers and/or hard drive capacity)
   d. Networking of desktop computers
   e. Information about operating systems for network servers, including model versions
   f. Details about creating, storing and retrieving of back up tapes (hard drives, servers, e-mail system)
   g. Details about disaster recovery procedure (software is used to convert back up tapes into usable format)

h. Details about facsimile machines used by deponent's employer and the procedures to use fax machines (e.g., fax logs, memory of fax machines)

3. Software and E-Mail:

   a. Details about application software used on desktops and laptops (including company standard software, such as Word, Excel, Power Point; length of time this software was company standard, what version)

   b. Details about company-approved/standards for personal digital assistants (*e.g.*, hand-held devices such as Palm Pilot)

   c. Details about e-mail system(s) used by deponent's employer (retention period, use of files, deletion procedures)

4. Record Management and Document Preservation:

   a. Notification and instructions about preservation of documents due to the lawsuit (who provided the notification, how was it communicated)

   b. Details of any deletion of documents since commencement of lawsuit or since deponent received notification about lawsuit or reasonable anticipation of lawsuit

   c. Details about company's record management policy (when instituted, when electronic documents became part of this policy, who is responsible for ongoing management (education, audit, enforcement) of this policy, provide copy during deposition)

   d. Determine if he/she has examined any computers since learning of this lawsuit; if yes, establish details about protocol IT person used

5. Alternative sources of electronic information:

   a. Identify any locations outside deponent's employer where electronic documents are regularly sent

   b. Names (and location, etc.) of persons who would have knowledge about 3rd party's computer systems
   c. Details about Internet site of employer (access by 3rd parties, content, who develops content, intervals for revision)

6. Backup Procedures:

   a. Details about company's backup procedures (including intervals, medium for backup, reuse of backup medium, location of backup)

   b. Since filing of lawsuit, has any backup tape been reused or otherwise erased (details about this)

7. Production of electronic documents in other lawsuits:

   a. Details about electronic production in other lawsuits (what cases, what was produced, format of production)

   b. Information about use of this electronic documentation in other litigation (at depositions, to support motions, at trial on merits)

8. Hardware:

   a. Details about disposal/recycling/sale of hardware (including what happens to hard drives)

9. Legacy Systems:

Details about software used for backup media or archived documentation (include information whether deponent retains legacy software and manuals)

ATTACHMENT 6

Sample Interrogatories

System Archaeology

[There are many computer systems and network configurations. It may be useful to learn more about your opponent's electronic systems before engaging in the core part of electronic discovery. These interrogatories will assist in gaining an overall idea of the opposition's computer systems and network configurations. These sample interrogatories may be narrowed to focus on smaller departments or operating groups within a department. These interrogatories will also be useful during interviews or depositions of key witnesses associated with the opposition's computer systems.]

1. Describe in detail the layout of the computer system, including, but not limited to, the number and type of computers and the type(s) of operating system(s) and application software packages used. [You will want as much detail as you can obtain about connectivity, names and versions of software programs used for electronic mail, calendars, project management files, word processing, and database management.]

2. For each of the following individuals [insert names] provide a detailed description of their computer(s), including desktop computers, personal digital assistances, portable, laptop and notebook computers. If an individual uses a computer for business purposes that is located at his/her residence, please include information concerning these systems. [You will want detailed information about each computer (and manufacturer and model); name and version of all software, including operating system, private and custom developed applications, commercial applications and shareware, communications capability, including, but not limited to, terminal to mainframe emulation, data download and/or upload capability to mainframe, and computer to computer connections via network, modem and/or direct connection.]

3. Provide the following information for each computer network in operation in the organization [You may want to limit this interrogatory to a particular department or subgroup]:

    a) Name and version number of the network operation system in use;

    b) Quantity and configuration of all network servers and workstations;

    c) Identity of the person(s) responsible for the ongoing operation, maintenance, expansion and upkeep of the network; and

    d) Name and version of all application and other software residing on the network, including, but not limited to, electronic mail applications.

4. Provide the following for each mini- and mainframe computer system used in the organization:

    a) Name and version number of the operating system in use;

    b) Identity of the person(s) responsible for the ongoing operation, maintenance, expansion and upkeep of the mini- and/or mainframe system; and

    c) Name and description of function of all application and other software residing on the network, including, but not limited to, electronic mail applications.

5. Describe in detail all possible ways in which electronic data are shared between organizations, the method of transmission, type(s) of data transferred and the names of all individual possessing the capability for such transfer, including lists and names of authorized regular outside users of the [producing party's] electronic mail system.

6. Please provide the following information concerning data backups performed on all computer systems in the organization:

    a) Descriptions of any and all procedures and/or devices used to backup the software and/or data, including, but not limited to, name(s) of backup software used, tape rotation schedule, type of tape backup drives including name and version number;

    b) Are multiple generations of backups maintained? If so, please describe now many and whether the backups are full or incremental;

    c) Are backup storage media kept off-site? If so, where are such media kept? Describe the process for archiving and retrieving off-site media?

    d) Are backup storage media kept on-site? If so, where are such media kept? Describe the process for archiving and retrieving on-site media;

    e) Identify who conducts the backup, including name, title, office location, and telephone number;

    f) Describe, in detail, what information is backed up; and

    g) Please provide a detailed list of all backup sets, regardless of the magnetic media on which they reside, showing current location, custodian, date of backup and a description of backup content.

In some litigation, voice mail messages may be important. These may be more difficult to gain access to due to technical limitations in the voice mail service.

7. State whether users may store voice mail messages. If so, please provide the following information:

    a) State whether users have the option of storing voice mail messages;

b) If users can store messages, state how long messages remain on the system? State how many messages may be stored by each user; and

c) State whether voice mail messages are automatically purged. If so, describe in detail the destruction schedule.

System Configuration:

1. Describe the types (including names and models) of computer system(s) used by your company in the course of business.
2. Describe/identify the name, type and version of software used on your computer system(s).
3. Identify the person(s) responsible for the ongoing operation, maintenance, expansion, backup and upkeep of the computer system.
4. Do employees have home computers used for business purposes? If yes, insert answers to questions 1-2 for computers used at home for business purposes.
5. Are passwords or encrypted files used on any of the computer systems?
    a. If yes, describe how files are protected
    b. Who could provide access codes if required?
    c. Have you modified your use of computers to comply with recent discovery requests?
    d. Have you deleted any files or other electronic documents since the filing of this lawsuit?

Backup and Retention:

1. List all computer systems in the organization that are backed up.
    a. Describe the backup program(s) used (including information about legacy systems).
    b. Give details of your backup procedures/protocols:
2. Have you modified or suspended your backup procedures/protocols to comply with recent discovery requests? If the answer is yes, please provide a detailed description of what has been done.
3. Are files ever deleted from the computer system(s) as part of backup/retention procedures?
4. Are archival backups ever created? If yes, what files have been archived? What are the archival backups maintained?
5. Describe any disaster recovery plans in place now and for the time period relevant to this lawsuit.

Maintenance and Access:

1. Are utility programs used on computer(s) in the office?
    a. If yes: Which programs?
    b. Has the program been used to permanently “wipe” files?
    c. If yes, when?
    d. Has the program been used to de-fragment, optimize or compress drives?
    e. If yes, when?
2. If persons outside of the company can access the company computers, how do those outside of the company access the computers?
3. How are office computers secured?
4. Has any computer hardware been upgraded in the past 12 months?
5. Has any computer software been upgraded or replaced on office computers in the past 12 months?

Chain of Custody/Authentication:

1. Are individual directories purged when an employee leaves the company?
2. Are passwords and access codes revoked when an employee leaves the company?
3. Are workstations reassigned to incoming employees?
    a. If yes, are hard drives wiped or re-formatted for the new user?
    b. Are hard drives backed up before the new user uses the workstation?
4. Describe how used or replaced equipment is disposed of or sold.
5. Describe how used disks or drives are treated before destruction or sale, including whether they are degaussed or shredded.
6. Have you used outside contractors to upgrade either hardware of software?
    a. If yes, please identify the contractors.
7. Are changes or modifications made to software recorded?

a. If yes, please describe the medium for recording, e.g., electronic.

b. Are hard copy logs kept?

Computer hardware:

1. List all computer equipment provided by [party name] or used by employees of [party name] to perform work for [party name], including but not limited to hardware/or peripherals attached to a computer such as computer cases [desktop, tower, portable/batteries, all-in-one], monitors, modems [internal, external], printers, keyboards, scanners, mice [cord and cordless], pointing devices [joystick, touch pad, trackball], speakers, include description of equipment, serial number, all users for the period _____to _____ and dates used, and all locations where the equipment was located for the period _____ to _____.

2. Will [party name] permit, without an order therefore, inspection of the equipment described in the answer to the preceding interrogatory?

3. List all hardware components (e.g., motherboard, modem, NIC, etc.) installed internally or externally to the PC(s) used by _____ during the period _____ to _____.

4. List discarded or replaced hardware and software for the PC(s) (including entire PCs) used by _____ during the period _____ to _____. If the hardware or software is no longer in your control, state the name and contact information of the last known custodian.

Computer Software:

1. List any and all software installed or used on the PC(s) used by _____ during the period _____ to _____. Include all titles and version numbers. Include authors and contact information for authors of custom or customized software. Include Operating System(s) software.

Operating Systems:

1. List all operating systems (including but not limited to UNIX, Windows, DOS, Linux, and PDA operating systems) installed on all computers used by [party name], the specific equipment the Operating System was installed on, and the period during which it was in stalled on the specific equipment.

Telephone or Communication Systems:

1. Do you have any graphic representation of the components of the telephone and voice messaging system of [party name], and the relationship of those components to each other, including but not limited to flow charts, videos, photos, or diagrams?

2. If so, where are the documents located?

3. List all telephone equipment provided by [party name] or used by employees of [party name] to perform work for [party name], including but not limited to desktop telephones, cellular phones, pagers, PDA and laptop modems, calling cards, telephony software, and contact management software. Include description of equipment and software, serial number, all users of the period of _____ to _____, and dates used, and all locations where the equipment was located for the period of _____ to _____ inclusive.

Other Sources of Electronic Evidence:

1. List all log files (files with suffixes but not limited to . . . found on computers in [party name]'s network, and the equipment and logical path where the log files may be found.
2. Do any employees of [party name] subscribe to or participate in Internet newsgroups or chat groups in the course of their employment?

3. If yes, list all users and the services that they subscribe to or participate in.

4. Do any employees of [party name] use portable devices in the course of their employment that are not connected to [party name]'s network and which are not backed up in archives?
5. If so, list all users and the devices they use.

6. Do any employees of [party name] use portable devices in the course of their employment that are not connected to [party name]'s network and which are not backed up in archives?
7. If so, list all users and the devices they use.

8. Does [party name] provide Internet access for any of its employees or has [party name] does so at any time during the period from _____ to _____inclusive/
9. If so, list the employees who had Internet access, the Internet service provide (ISP) used, and describe the method(s) used to connect to the Internet.

10. Describe any restrictions on, controls over, or monitoring of employee use of Internet resources.

11. Provide a list of any and all Internet-related data on the PCs used by [specific employees or classes of employees], including but not limited to save web pages, lists of web sites, URL addresses, Web browser software and settings, bookmarks, favorites, history lists, caches, cookies.

Data Security Measures:

1. List any and all user identification numbers and passwords necessary to access computers or programs addressed in interrogatories. Your response to this Interrogatory must be updated with responses to future sets of Interrogatories and updated responses to any set of Interrogatories.

2. Explain [party name]'s policies and procedures for protecting data.

3. Explain [party name]'s policy for application specific security settings.

Network Questions:

1. List any and all documents and things related to networks or groups of connected computers that allow people to share information and equipment, including but not limited to local area networks (LAN), wide area networks (WAN), metropolitan area networks (MAN), storage area networks (SAN), peer-to-peer networks, client-server networks, integrated services digital networks, virtual private networks (VPN).

2. List any and all documents related to networks, including but not limited to information exchange components (e.g., Ethernet, token-ring, ATM), network file servers, traffic, hubs, network interface cards, cables, firewalls, user names, passwords, Intranet.

3. Do you have any graphic representation of the components of your computer network, and the relationship of those components to each other, including but not limited to flow charts, videos, photos, or drawings.

4. If so, where are the documents located. Include logical paths for electronic documents.

5. List any and all information related to e-mail, including but not limited to, current, backed up and archived programs, accounts, unified messaging, server-based e-mail, web-based e-mail, dial-up e-mail, user names and addresses, domain names and addresses, e-mail messages, attachments, manual and automated mailing lists, mailing list addresses.

ATTACHMENT 7

IN THE FEDERAL DISTRICT COURT
FOR THE DISTRICT OF _____

[. . . .], Plaintiff,	)	
v.	)	C.A. No. _____
[. . . .], Defendant.	)	

[PLAINTIFF/DEFENDANT'S] MOTION TO PERMIT INSPECTION AND COPYING OF COMPUTER STORAGE DEVICES OR TO COMPEL PRODUCTION OF COMPUTER EQUIPMENT BY [DEFENDANT/PLAINTIFF]

Pursuant to Federal Rule of Civil Procedure 37 generally and 37(a)(2)(B) specifically and upon reasonable notice to [Defendant/Plaintiff], [Plaintiff/Defendant] moves this Court to permit inspection and copying of computer storage devices in accordance with [Plaintiff's/Defendant's] Request for Production of Documents and Things and/or to compel production of computer equipment, software and documents by [Defendant/Plaintiff] for inspection and copying. [Plaintiff/Defendant] respectfully requests that this Court enter an Order (Attachment A) directing [Defendant/Plaintiff] to produce for inspection and copying, within five (5) business days of the Order, certain computer equipment, computer storage devices, software and documents used by [Defendant/Plaintiff] during the time period relevant to the actions taken that constitute the basis for this lawsuit.

BACKGROUND

On _____, counsel for [Plaintiff/Defendant] sent a letter to [Defendant/Plaintiff] informing that [Plaintiff/Defendant] electronic data or compilations would

be an important and irreplaceable source for discovery and/or evidence and that [Plaintiff/ Defendant] intended to submit discovery requests to obtain documents and other information in electronic form and to access computer(s), computer network(s) and computer systems. (Attachment B) This letter reminded [Defendant/Plaintiff] that his/her obligation to preserve electronic data is the same as for other forms of evidence. Counsel for [Plaintiff/ Defendant] requested that [Defendant/Plaintiff] safeguard against the destruction of evidence until final resolution of the litigation and listed eight categories of electronic data that should be preserved.

After receipt of this letter and after commencement of this lawsuit, [Defendant/Plaintiff] has embarked on a course of conduct designed to hinder and delay and even destroy evidence that is relevant to this lawsuit. [For example, [Defendant's/Plaintiff's] records management program was not suspended and electronic documents have been deleted, or in the normal course of [Defendant's/Plaintiff's] ongoing disaster recovery program systems administrators have reused critical backup tapes and thereby overwritten discoverable information, or files have been deleted from the hard drives of critical desktop or laptop computers].

As part of the discovery in this lawsuit, [Plaintiff/Defendant] served a set of Requests for Production of Computer Equipment, electronic documents, software, and other items upon [Defendant/Plaintiff]. Each of the requests is narrow and directed to the issues relevant to this lawsuit, and none is overbroad or burdensome. [Defendant/Plaintiff] has refused to produce responsive material on the grounds that the requests are vague, ambiguous, overly broad and burdensome, and because they seek confidential and proprietary documents, as well as documents protected by attorney-client and work-product privileges. Since the filing of this lawsuit, [Defendant/Plaintiff] has knowingly permitted or contributed to the destruction of responsive evidence.

Counsel for [Plaintiff/Defendant] sent a letter to opposing counsel proposing a procedure to access [Defendant's/Plaintiff's] computers and servers. The procedure incorporated the parties' agreed Confidentiality Order for protection of attorney-client and work product privileges and protection of trade secrets and proprietary information. The procedure proposed by counsel provided:

1. Defendants and counsel will meet with plaintiffs' counsel with computer forensic expert and review each file on computer. This review will be conducted in a manner that does not disrupt plaintiffs' business.

2. If a file may lead to discovery of admissible evidence and is not protected from production by a privilege, it will be copied and produced.

3. A privilege log will be maintained of all documents withheld on basis of privilege.

4. If the parties conclude file may not lead to discovery of admissible evidence, it will not be produced.

5. Plaintiffs will use and pay for their own expert for this process. If defendants want a neutral expert, costs for the neutral expert will be shared equally.

Counsel for [Defendant/Plaintiff] rejected this proposal.

ARGUMENT

[Plaintiff/Defendant] put [Defendant/Plaintiff] on notice at the outset of this lawsuit that discovery would include electronic versions of documents. A party's duty to preserve relevant documents arises when a party reasonably anticipates litigation. *Zubulake v. UBS Warburg* ("*Zubulake* I"), 220 F.R.D. 212, 217 (S.D.N.Y. 2003); *Renda Marine, Inc. v. United States*, 58 Fed. Cl. 57, 61 (Fed. Cl. 2003); *see* Civil Discovery Standards, ABA Section of Litigation, at part IV, page 17 (August 2004).

[Plaintiff/Defendant] has a duty to suspend its ongoing records management or the reuse of backup tapes once the duty to preserve documents arises. *Lewy v. Remington Arms Co.*, 836 F.2d 1104 (8th Cir. 1988); *Applied Telematics, Inc. v. Sprint Communications Co*., 1996 U.S. Dist. LEXIS 14053 (E.D.Pa. September 17, 1996);

[Plaintiff/Defendant] has no means to obtain the full content of documents prepared with the use of computer equipment other than by inspection of the equipment itself.

Under Federal Rule of Civil Procedure 26(b)(2)(i)-(iii), the interests of [Plaintiff/Defendant] outweigh those of [Defendant/Plaintiff]. *See Fennell v. First Step Designs*, 83 F.3d 526 (1st Cir. 1996). [Defendant/Plaintiff] will suffer no undue burden or prejudice from being required to comply with [Plaintiff's/Defendant's] document production request. On the other hand, absent compliance by [Defendant/Plaintiff] with its discovery obligations, [Plaintiff/Defendant] will be unable to effectively pursue its claims against [Defendant/Plaintiff] because, due to the inexcusable conduct of [Defendant/Plaintiff] relevant, material and non-privileged information will have been withheld from [Plaintiff/Defendant].

Federal Rule of Civil Procedure 34(a) provides, in pertinent part, that "[a]ny party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect and copy, any designated documents (including . . . data compilations)." *Bills v. Kennecott Corp.*, 108 F.R.D. 459 (D.Utah 1985).

The obligation to produce electronic versions of documents and records is not new. Since 1970, Federal Rule of Civil Procedure 34 has authorized a party to request production of designated documents in electronic form and the electronic source itself. Advisory Committee Notes for the 1970 Amendments to Rule 34; *Illinois Tool Works v. Metro Mark Products*, 43 F.Supp.2d 951 (N.D.Ill. 1999). The Rules will be amended again, effective December 1, 2006. Amended Rule 34 states that "electronically stored information" … "must be produced forms in which it is ordinarily maintained, or" in a "reasonably usable" form. FED. R. CIV. PRO. 34(a)

The electronic version of a document contains valuable information that the hard copy does not provide. In *Armstrong v. Executive Office of the President*, 1 F.3d 1274 (D.C.Cir. 1993), the court said that printing a hard copy of an e-mail message was not the same as preserving the electronic version because the hard copy does not contain directories, distribution lists, acknowledgment of receipts, or transmittal information. In *Williams v. Sprint/United Mgmt. Co.*, 230 F. R. D. 640 (D. Kan. 2005), in a discussion about production of documents in its native format, the court stated that a database application, for example, "contains an undifferentiated mass of tables of data. The metadata is the key to showing the relationships between the data; without such metadata, the tables of data would have little meaning." *Id*. at 647. "A spreadsheet's metadata may be necessary to understand the spreadsheet because the cells containing formulas … often display a value rather than the formula itself. To understand the spreadsheet, the user must be able to ascertain the formula within the cell." *Id.*

Numerous recent court decisions have ruled that Rule 34 permits party to request production of a document in its electronic form and not merely rely on the hard copy of a document. In *Playboy Enterprises v. Welles*, 60 F.Supp.2d 1050 (S.D.Cal. 1999), plaintiff requested access to defendant's hard drive to attempt to recover deleted files that may have been stored on the hard drive. The court determined that plaintiff's need for access outweighed the potential interruption to defendant's business and approved plaintiff's request. In *TY, Inc. v. Le Claire*, 2000 WL 1015934 (N.D.Ill. June 1, 2000), the court granted plaintiff's motion and authorized plaintiff, at its own expense, to inspect the hard drives of computers defendants used during the relevant time period. In *Simon Property Group v. mySimon,*, 194 F.R.D. 639 (S.D. Ind. 2000), the court granted plaintiff's motion to compel defendants to produce their computers so that plaintiffs could attempt to recover deleted computer files.

RELIEF REQUESTED

For these reasons stated, [Plaintiff/Defendant] respectfully requests that this Court enter an Order directing [Defendant/Plaintiff] to permit inspection and copying of certain computer equipment, computer storage devices, software and documents used by [Defendant/Plaintiff] during the time period relevant to the actions taken that constitute the basis for this lawsuit and directing [Defendant/Plaintiff] produce the designated computer equipment, software and documents within five (5) business days of this Order.

ATTACHMENT 8

Draft Engagement Letter for Computer Forensic Expert

Privileged & Confidential
Prepared In Connection With Litigation

[Addressee Information]

RE: [Case Name, Number and Court]

Dear _____:

This letter confirms the terms and conditions of [name of law firm] engagement to retain your services as an expert on behalf of [insert name of party(ies)] in this case. We represent this party in the litigation.

We have engaged you as both a consultant and expert witness regarding (1) the recovery and/or reconstruction of certain electronic data (including certain e-mail messages and attachments to these messages) contained on the hard drive of [insert name of person who uses or owns the desktop or laptop computer] [additional personal computers may be similarly identified and included] and (2) the analysis of such data (including but not limited to metadata such as original author, date and time of creation, how document may have been edited and routed). There may be additional topics in this litigation on which we will request your expert evaluation and opinion. Your work in connection with these additional topics will be subject to the terms of this engagement. You will prepare an expert report summarizing your work, findings, and opinion. This report will have to be completed by the date set by the Court's discovery schedule. You should expect to be deposed concerning your forensic work.

We and [name of firm's client] are your confidential clients. You will take all reasonable steps to ensure that you and your firm do not disclose any information pertaining to your services under this engagement and this lawsuit any one other than to this firm or [name of person employed by firm's client]. Your work pursuant to this engagement is subject to the attorney-client and attorney-work product privileges, and any other privilege that may apply. All documents you prepare, including drafts of your expert report, in connection with this engagement should be conspicuously marked with the legend: "**Privileged and Confidential – Prepared At the Direction of Counsel In Connection With Litigation**." If a protective order is issued in this litigation, we will ask you to sign a copy of this order and be bound by its terms.

We will pay you a flat fee of [$ insert the amount] per hard drive for your computer forensic analysis of the electronic data on each hard drive examined and for transferring that electronic data to a CD disc or floppy disk for our use. We will also pay you an hourly rate of $ [insert amount] for the preparation of your expert report, preparation of any affidavits or declarations that we may require in the course of this lawsuit, preparation for your testimony at a deposition and/or trial, and your actual testimony. We will reimburse you for your reasonable and actual out-of-pocket expenses (including mileage). Please submit monthly invoices with detailed descriptions of your daily activities and hours spent. We will review your invoices for accuracy and reasonableness and forward them to [name of client] for payment.

Your compliance (or the compliance of your firm) with a court order (or administrative order) to testify and/or to produce documents will not be a breach of the confidentiality provisions of this engagement. You agree to provide prompt notice to counsel if any such order is served upon you or your firm. Your further agree that you will cooperate fully in any efforts we undertake (or client's name) undertakes to oppose such order. In the event that we or our client requires you or your firm to take any legal action to protect against disclosure of information or materials, we will either represent you, engage another firm to represent you, or indemnify and hold you and your firm harmless for reasonable attorney's fees, costs and expenses that may result from the legal action you undertake.

You represent that there are no conflicts of interest between you and your organization, on the one hand, and our client, our firm, our opponent and our opponent's law firm.

Please review this engagement letter. If it fairly represents the terms for our engaging your services in connection with this lawsuit, please sign and date the original and return it to me by overnight delivery.

If you have any questions about the terms of this engagement, please contact me.

Very truly yours,

FEDERAL RULES OF CIVIL PROCEDURE

Rule 16. Pretrial Conferences; Scheduling; Management

* * * * *

(b) Scheduling and Planning. Except in categories of actions exempted by district court rule as inappropriate, the district judge, or a magistrate judge when authorized by district court rule, shall, after receiving the report from the parties under Rule 26(f) or after consulting with the attorneys for the parties and any unrepresented parties by a scheduling conference, telephone, mail, or other suitable means, enter a scheduling order that limits the time

(1) to join other parties and to amend the pleadings;

(2) to file motions; and

(3) to complete discovery.

The scheduling order also may include

(4) modifications of the times for disclosures under Rules 26(a) and 26(e)(1) and of the extent of discovery to be permitted;

(5) provisions for disclosure or discovery of electronically stored information;

(6) any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after production;

(75) the date or dates for conferences before trial, a final pretrial conference, and trial; and

(86) any other matters appropriate in the circumstances of the case.

The order shall issue as soon as practicable but in any event within 90 days after the appearance of a defendant and within 120 days after the complaint has been served on a defendant. A schedule shall not be modified except upon a showing of good cause and by leave of the district judge or, when authorized by local rule, by a magistrate judge.

* * * * *

Committee Note

The amendment to Rule 16(b) is designed to alert 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. Rule 26(f) is amended to direct the parties to discuss discovery of electronically stored information if such discovery is contemplated in the action. Form 35 is amended to call for a report to the court about the results of this discussion. In many instances, the court's involvement early in the litigation will help avoid difficulties that might otherwise arise.

Rule 16(b) is also amended to include among the topics that may be addressed in the scheduling order any agreements that the parties reach to facilitate discovery by minimizing the risk of waiver of privilege or work-product protection. Rule 26(f) is amended to add to the discovery plan the parties' proposal for the court to enter a case-management or other order adopting such an agreement. The parties may agree to various arrangements. For example, they may agree to initial provision of requested materials without waiver of privilege or protection to enable the party seeking production to designate the materials desired or protection for actual production, with the privilege review of only those materials to follow. Alternatively, they may agree that if privileged or protected information is inadvertently produced, the producing party may by timely notice assert the privilege or protection and obtain return of the materials without waiver. Other arrangements are possible. In most circumstances, a party who receives information under such an arrangement cannot assert that production of the information waived a claim of privilege or of protection as trial-preparation material.

An order that includes the parties' agreement may be helpful in avoiding delay and excessive cost in discovery. *See Manual for Complex Litigation* (4th) § 11.446. Rule 16(b)(6) recognizes the propriety of including such agreements in the court's order. The rule does not provide the court with authority to enter such a case-management or other order without party agreement, or limit the court's authority to act on motion.

Changes Made After Publication and Comment

This recommendation is of a modified version of the proposal as published. Subdivision (b)(6) was modified to eliminate the references to "adopting" agreements for "protection against waiving" privilege. It was feared that these words might seem to promise greater protection than can be assured. In keeping with changes to Rule 26(b)(5)(B), subdivision (b)(6) was expanded to include agreements for asserting claims of protection as trial-preparation materials. The Committee Note was revised to reflect the changes in the rule text.

The proposed changes from the published rule are set out below.

Rule 16. Pretrial Conferences; Scheduling; Management*

* * * * *

(b) Scheduling and Planning.

* * * * *

The scheduling order may also include

* * * * *

(6) ~~adoption of the parties'~~ any agreements the parties reach for ~~protection against waiving~~ asserting claims of privilege or of protection as trial-preparation material after production;

* * * * *

Rule 26(a)

The Committee recommends approval of the following amendment:

Rule 26. General Provisions Governing Discovery; Duty of Disclosure

(a) Required Disclosures; Methods to Discover Additional Matter.

(1) ***Initial Disclosures.*** Except in categories of proceedings specified in Rule 26(a)(1)(E), or to the extent otherwise

*Changes from the proposal published for public comment shown by double-underlining new material and striking through omitted matter.

stipulated or directed by order, a party must, without awaiting a discovery request, provide to other parties:

(A) the name and, if known, the address and telephone number of each individual likely to have discoverable information that the disclosing party may use to support its claims or defenses, unless solely for impeachment, identifying the subjects of the information;

(B) a copy of, or a description by category and location of, all documents, electronically stored information, ~~data compilations~~, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment;

* * * * *

Committee Note

Subdivision (a). Rule 26(a)(1)(B) is amended to parallel Rule 34(a) by recognizing that a party must disclose electronically stored information as well as documents that it may use to support its claims or defenses. The term "electronically stored information" has the same broad meaning in Rule 26(a)(1) as in Rule 34(a). This amendment is consistent with the 1993 addition of Rule 26(a)(1)(B). The term "data compilations" is deleted as unnecessary because it is a subset of both documents and electronically stored information.

Changes Made After Publication and Comment

As noted in the introduction, this provision was not included in the published rule. It is included as a conforming amendment, to make Rule 26(a)(1) consistent with the changes that were included in the published proposals.

Rule 26(f)

The Committee recommends approval of the following amendments to Rule 26(f).

Rule 26. General Provisions Governing Discovery; Duty of Disclosure

* * * * *

(f) Conference of Parties; Planning for Discovery. Except in categories of proceedings exempted from initial disclosure under Rule 26(a)(1)(E) or when otherwise ordered, the parties must, as soon as practicable and in any event at least 21 days before a scheduling conference is held or a scheduling order is due under Rule 16(b), confer to consider the nature and basis of their claims and defenses and the possibilities for a prompt settlement or resolution of the case, to make or arrange for the disclosures required by Rule 26(a)(1), to discuss any issues relating to preserving discoverable information, and to develop a proposed

discovery plan that indicates the parties' views and proposals concerning:

(1) what changes should be made in the timing, form, or requirement for disclosures under Rule 26(a), including a statement as to when disclosures under Rule 26(a)(1) were made or will be made;

(2) the subjects on which discovery may be needed, when discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused upon particular issues;

(3) any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced;

(4) any issues relating to claims of privilege or of protection as trial-preparation material, including — if the parties agree on a procedure to assert such claims after production — whether to ask the court to include their agreement in an order;

(53) what changes should be made in the limitations on discovery imposed under these rules or by local rule, and what other limitations should be imposed; and

(64) any other orders that should be entered by the court under Rule 26(c) or under Rule 16(b) and (c).

* * * * *

Committee Note

Subdivision (f). Rule 26(f) is amended to direct the parties to discuss discovery of electronically stored information during their discovery-planning conference. The rule focuses on "issues relating to disclosure or discovery of electronically stored information"; the discussion is not required in cases not involving electronic discovery, and the amendment imposes no additional requirements in those cases. When the parties do anticipate disclosure or discovery of electronically stored information, discussion at the outset may avoid later difficulties or ease their resolution.

When a case involves discovery of electronically stored information, the issues to be addressed during the Rule 26(f) conference depend on the nature and extent of the contemplated discovery and of the parties' information systems. It may be important for the parties to discuss those systems, and accordingly important for counsel to become familiar with those systems before the conference. With that information, the parties can develop a discovery plan that takes into account the capabilities of their computer systems. In appropriate cases identification of, and early discovery from, individuals with special knowledge of a party's computer systems may be helpful.

The particular issues regarding electronically stored information that deserve attention during the discovery planning stage depend on the specifics of the given case. *See Manual for Complex Litigation* (4th) § 40.25(2) (listing topics for discussion in a proposed order regarding meet-and-confer sessions). For example, the parties may specify the

topics for such discovery and the time period for which discovery will be sought. They may identify the various sources of such information within a party's control that should be searched for electronically stored information. They may discuss whether the information is reasonably accessible to the party that has it, including the burden or cost of retrieving and reviewing the information. *See* Rule 26(b)(2)(B). Rule 26(f)(3) explicitly directs the parties to discuss the form or forms in which electronically stored information might be produced. The parties may be able to reach agreement on the forms of production, making discovery more efficient. Rule 34(b) is amended to permit a requesting party to specify the form or forms in which it wants electronically stored information produced. If the requesting party does not specify a form, Rule 34(b) directs the responding party to state the forms it intends to use in the production. Early discussion of the forms of production may facilitate the application of Rule 34(b) by allowing the parties to determine what forms of production will meet both parties' needs. Early identification of disputes over the forms of production may help avoid the expense and delay of searches or productions using inappropriate forms.

Rule 26(f) is also amended to direct the parties to discuss any issues regarding preservation of discoverable information during their conference as they develop a discovery plan. This provision applies to all sorts of discoverable information, but can be particularly important with regard to electronically stored information. The volume and dynamic nature of electronically stored information may complicate preservation obligations. The ordinary operation of computers involves both the automatic creation and the automatic deletion or overwriting of certain information. Failure to address preservation issues early in the litigation increases uncertainty and raises a risk of disputes.

The parties' discussion should pay particular attention to the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities. Complete or broad cessation of a party's routine computer operations could paralyze the party's activities. *Cf. Manual for Complex Litigation* (4th) § 11.422 ("A blanket preservation order may be prohibitively expensive and unduly burdensome for parties dependent on computer systems for their day-to-day operations.") The parties should take account of these considerations in their discussions, with the goal of agreeing on reasonable preservation steps.

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(f) is also amended to provide that the parties should discuss any issues relating to assertions of privilege or of protection as trial-preparation materials, including whether the parties can facilitate discovery by agreeing on procedures for asserting claims of privilege or protection after production and whether to ask the court to enter an order that includes any agreement the parties reach. The Committee has repeatedly been advised about the discovery difficulties that can result from efforts to guard against waiver of privilege and work-product protection. Frequently parties find it necessary to spend large amounts of time reviewing materials requested through discovery to avoid waiving privilege. These efforts are necessary because materials subject to a claim of privilege or protection are often difficult to identify. A failure to withhold even one such item may result in an argument that there has been a waiver of privilege as to all other privileged materials on that subject matter. Efforts to avoid the risk of waiver can impose substantial costs on the party producing the material and the time required for the privilege review can substantially delay access for the party seeking discovery.

These problems often become more acute when discovery of electronically stored information is sought. The volume of such data, and the informality that attends use of e-mail and some other types of electronically stored information, may make privilege determinations more difficult, and privilege review correspondingly more expensive and time consuming. Other aspects of electronically stored information pose particular difficulties for privilege review. For example, production may be sought of information automatically included in electronic files but not apparent to the creator or to readers. Computer programs may retain draft language, editorial comments, and other deleted matter (sometimes referred to as "embedded data" or "embedded edits") in an electronic file but not make them apparent to the reader. Information describing the

history, tracking, or management of an electronic file (sometimes called "metadata") is usually not apparent to the reader viewing a hard copy or a screen image. Whether this information should be produced may be among the topics discussed in the Rule 26(f) conference. If it is, it may need to be reviewed to ensure that no privileged information is included, further complicating the task of privilege review.

Parties may attempt to minimize these costs and delays by agreeing to protocols that minimize the risk of waiver. They may agree that the responding party will provide certain requested materials for initial examination without waiving any privilege or protection — sometimes known as a "quick peek." The requesting party then designates the documents it wishes to have actually produced. This designation is the Rule 34 request. The responding party then responds in the usual course, screening only those documents actually requested for formal production and asserting privilege claims as provided in Rule 26(b)(5)(A). On other occasions, parties enter agreements — sometimes called "clawback agreements" — that production without intent to waive privilege or protection should not be a waiver so long as the responding party identifies the documents mistakenly produced, and that the documents should be returned under those circumstances. Other voluntary arrangements may be appropriate depending on the circumstances of each litigation. In most circumstances, a party who receives information under such an arrangement cannot assert that production of the information waived a claim of privilege or of protection as trial-preparation material.

Although these agreements may not be appropriate for all cases, in certain cases they can facilitate prompt and economical discovery by reducing delay before the discovering party obtains access to documents, and by reducing the cost and burden of review by the producing party. A case-management or other order including such agreements may further facilitate the discovery process. Form 35 is amended to include a report to the court about any agreement regarding protections against inadvertent forfeiture or waiver of privilege or protection that the parties have reached, and Rule 16(b) is amended to recognize that the court may include such an agreement in a case-management or other order. If the parties agree to entry of such an order, their proposal should be included in the report to the court.

Rule 26(b)(5)(B) is added to establish a parallel procedure to assert privilege or protection as trial-preparation material after production, leaving the question of waiver to later determination by the court.

Changes Made After Publication and Comment

The Committee recommends a modified version of what was published. Rule 26(f)(3) was expanded to refer to the form "or forms" of production, in parallel with the like change in Rule 34. Different forms may be suitable for different sources of electronically stored information.

The published Rule 26(f)(4) proposal described the parties' views and proposals concerning whether, on their agreement, the court should enter an order protecting the right to assert privilege after production. This has been revised to refer to the parties' views and proposals concerning any issues relating to claims of privilege, including — if the parties agree on a procedure to assert such claims after production — whether to ask the court to include their agreement in an order. As with Rule 16(b)(6), this change was made to avoid any implications as to the scope of the protection that may be afforded by court adoption of the parties' agreement.

Rule 26(f)(4) also was expanded to include trial-preparation materials.

The Committee Note was revised to reflect the changes in the rule text.

The changes from the published rule are shown below.

"bury" information that is necessary or useful for business purposes or that regulations or statutes require them to retain. Moreover, the 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.

The Proposed Rule and Committee Note

Rule 26(b)(2)

The Committee recommends approval of the following amendment:

Rule 26. General Provisions Governing Discovery; Duty of Disclosure

* * * * *

(b) Discovery Scope and Limits. Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows:

* * * * *

(2) Limitations.

(A) By order, the court may alter the limits in these rules on the number of depositions and interrogatories or the length of depositions under Rule 30. By order or local rule, the court may also limit the number of requests under Rule 36.

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

(C) The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the

amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues. The court may act upon its own initiative after reasonable notice or pursuant to a motion under Rule 26(c).

* * * * *

Committee Note

Subdivision (b)(2). The amendment to Rule 26(b)(2) is designed to address issues raised by difficulties in locating, retrieving, and providing discovery of some electronically stored information. Electronic storage systems often make it easier to locate and retrieve information. These advantages are properly taken into account in determining the reasonable scope of discovery in a particular case. But some sources of electronically stored information can be accessed only with substantial burden and cost. In a particular case, these burdens and costs may make the information on such sources not reasonably accessible.

It is not possible to define in a rule the different types of technological features that may affect the burdens and costs of accessing electronically stored information. Information systems are designed to provide ready access to information used in regular ongoing activities. They also may be designed so as to provide ready access to information that is not regularly used. But a system may retain information on sources that are accessible only by incurring substantial burdens or costs. Subparagraph (B) is added to regulate discovery from such sources.

Under this rule, a responding party should produce electronically stored information that is relevant, not privileged, and reasonably accessible, subject to the (b)(2)(C) limitations that apply to all discovery. The responding party must also identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing. The identification should, to the extent possible, provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources.

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. It is often useful for the parties to discuss this issue early in discovery.

The volume of — and the ability to search — much electronically stored information means that in many cases the responding party will be able to produce information from reasonably accessible sources that will fully satisfy the parties' discovery needs. In many circumstances the requesting party should obtain and evaluate the information from such sources before insisting that the responding party search and produce information contained on sources that are not reasonably accessible. If the requesting party continues to seek discovery of information from sources identified as not reasonably accessible, the parties should discuss the burdens and costs of accessing and retrieving the information, the needs that may establish good cause for requiring all or part of the requested discovery even if the information sought is not reasonably accessible, and conditions on obtaining and producing the information that may be appropriate.

If the parties cannot agree whether, or on what terms, sources identified as not reasonably accessible should be searched and discoverable information produced, the issue may be raised either by a motion to compel discovery or by a motion for a protective order. The parties must confer before bringing either motion. If the parties do not resolve the issue and the court must decide, the responding party must show that the identified sources of information are not reasonably accessible because of undue burden or cost. The requesting party may need discovery to test this assertion. Such discovery might take the form of requiring the responding party to conduct a sampling of information contained on the sources identified as not reasonably accessible; allowing

some form of inspection of such sources; or taking depositions of witnesses knowledgeable about the responding party's information systems.

Once it is shown that a source of electronically stored information is not reasonably accessible, the requesting party may still obtain discovery by showing good cause, considering the limitations of Rule 26(b)(2)(C) that balance the costs and potential benefits of discovery. The decision whether to require a responding party to search for and produce information that is not reasonably accessible depends not only on the burdens and costs of doing so, but also on whether those burdens and costs can be justified in the circumstances of the case. Appropriate considerations may include: (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources.

The responding party has the burden as to one aspect of the inquiry — whether the identified sources are not reasonably accessible in light of the burdens and costs required to search for, retrieve, and produce whatever responsive information may be found. The requesting party has the burden of showing that its need for the discovery outweighs the burdens and costs of locating, retrieving, and producing the information. In some cases, the court will be able to determine whether the identified sources are not reasonably accessible and whether the requesting party has shown good cause for some or all of the discovery, consistent with the limitations of Rule 26(b)(2)(C), through a single proceeding or presentation. The good-cause determination, however, may be complicated because the court and parties may know little about what information the sources identified as not reasonably accessible might contain, whether it is relevant, or how valuable it may be to the litigation. In such cases, the parties may need some focused discovery, which may include sampling of the sources, to learn more about what burdens and costs are involved in accessing the information, what the information consists of, and how valuable it is for the litigation in light of information that can be obtained by exhausting other opportunities for discovery.

The good-cause inquiry and consideration of the Rule 26(b)(2)(C) limitations are coupled with the authority to set conditions for discovery. The conditions may take the form of limits on the amount, type, or sources of information required to be accessed and produced. The conditions may also include payment by the requesting party of part or all of the reasonable costs of obtaining information from sources that are not reasonably accessible. 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. But the producing party's burdens in reviewing the information for relevance and privilege may weigh against permitting the requested discovery.

The limitations of Rule 26(b)(2)(C) continue to apply to all discovery of electronically stored information, including that stored on reasonably accessible electronic sources.

Changes Made after Publication and Comment

This recommendation modifies the version of the proposed rule amendment as published. Responding to comments that the published proposal seemed to require identification of information that cannot be identified because it is not reasonably accessible, the rule text was clarified by requiring identification of sources that are not reasonably accessible. The test of reasonable accessibility was clarified by adding "because of undue burden or cost."

The published proposal referred only to a motion by the requesting party to compel discovery. The rule 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.

The provision that the court may for good cause order discovery from sources that are not reasonably accessible is expanded in two ways. It now states specifically that the requesting party is the one who must

show good cause, and it refers to consideration of the limitations on discovery set out in present Rule 26(b)(2)(i), (ii), and (iii).

The published proposal was added at the end of present Rule 26(b)(2). It has been relocated to become a new subparagraph (B), allocating present Rule 26(b)(2) to new subparagraphs (A) and (C). The Committee Note was changed to reflect the rule text revisions. It also was shortened. The shortening was accomplished in part by deleting references to problems that are likely to become antique as technology continues to evolve, and in part by deleting passages that were at a level of detail better suited for a practice manual than a Committee Note.

The changes from the published proposed amendment to Rule 26(b)(2) are set out below.

Rule 26. General Provisions Governing Discovery; Duty of Disclosure*

(b) Discovery Scope and Limits. Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows:

* * * * *

(2) Limitations.

* * * * *

*Changes from the proposal published for public comment shown by double-underlining new material and striking through omitted matter.

(B) A party need not provide discovery of electronically stored information from sources that had been disclosed to a nonparty, the absence of such language emerged as a concern during the comment period. The Committee decided to address this issue in the rule text, but to limit any such obligation to "reasonable steps" to retrieve such information. Such a formulation provides appropriate protection for the party asserting the claim pending its resolution, but also limits the burden on the receiving party.

The Committee specifically sought reaction during the comment period on whether to require the party that received the notice to certify compliance with the rule. There was little support for this addition during the comment period. One concern was that by requiring the creation of a new, separate document, such a provision would go beyond the certification that Rule 26(g) reads into the signature on a discovery document. Imposing an added requirement on a party that did not make the mistake precipitating the problem in the first place also raised concerns. The Committee decided not to include a certification requirement in the rule.

The Proposed Rule and Committee Note

Rule 26(b)(5)(B)

The Committee recommends approval of the following proposed amendment.

Rule 26. General Provisions Governing Discovery; Duty of Disclosure

* * * * *

(b) Discovery Scope and Limits. Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows:

* * * * *

(5) Claims of Privilege or Protection of Trial Preparation Materials.

(A) Information Withheld. When 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.

(B) Information Produced. If information is produced in discovery that is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved.

* * * * *

Committee Note

Subdivision (b)(5). The Committee has repeatedly been advised that the risk of privilege waiver, and the work necessary to avoid it, add to the costs and delay of discovery. When the review is of electronically stored information, the risk of waiver, and the time and effort required to avoid it, can increase substantially because of the volume of electronically stored information and the difficulty in ensuring that all information to be produced has in fact been reviewed. Rule 26(b)(5)(A) provides a procedure for a party that has withheld information on the basis of privilege or protection as trial-preparation material to make the claim so that the requesting party can decide whether to contest the claim and the court can resolve the dispute. Rule 26(b)(5)(B) is added to provide a procedure for a party to assert a claim of privilege or trial-preparation material protection after information is produced in discovery in the action and, if the claim is contested, permit any party that received the information to present the matter to the court for resolution.

Rule 26(b)(5)(B) does not address whether the privilege or protection that is asserted after production was waived by the production. The courts have developed principles to determine whether, and under what circumstances, waiver results from inadvertent production of privileged or protected information. Rule 26(b)(5)(B) provides a procedure for presenting and addressing these issues. Rule 26(b)(5)(B) works in tandem with Rule 26(f), which is amended to direct the parties to discuss privilege issues in preparing their discovery plan, and which, with amended Rule 16(b), allows the parties to ask the court to include in an order any agreements the parties reach regarding issues of privilege or trial-preparation material protection. Agreements reached under Rule 26(f)(4) and orders including such agreements entered under Rule 16(b)(6) may be considered when a court determines whether a waiver has occurred. Such agreements and orders ordinarily control if they adopt procedures different from those in Rule 26(b)(5)(B).

A party asserting a claim of privilege or protection after production must give notice to the receiving party. That notice should be in writing unless the circumstances preclude it. Such circumstances could include the assertion of the claim during a deposition. The notice should be as specific as possible in identifying the information and stating the basis for the claim. Because the receiving party must decide whether to challenge the claim and may sequester the information and submit it to the court for a ruling on whether the claimed privilege or protection applies and whether it has been waived, the notice should be sufficiently detailed so as to enable the receiving party and the court to understand the basis for the claim and to determine whether waiver has occurred. Courts will continue to examine whether a claim of privilege or protection was made at a reasonable time when delay is part of the waiver determination under the governing law.

After receiving notice, each party that received the information must promptly return, sequester, or destroy the information and any copies it has. The option of sequestering or destroying the information is included in part because the receiving party may have incorporated the information in protected trial-preparation materials. No receiving party may use or disclose the information pending resolution of the privilege claim. The receiving party may present to the court the questions whether the information is privileged or protected as trial-preparation material, and whether the privilege or protection has been waived. If it does so, it must provide the court with the grounds for the privilege or protection specified in the producing party's notice, and serve all parties. In presenting the question, the party may use the content of the information only to the extent permitted by the applicable law of privilege, protection for trial-preparation material, and professional responsibility.

If a party disclosed the information to nonparties before receiving notice of a claim of privilege or protection as trial-preparation material, it must take reasonable steps to retrieve the information and to return it, sequester it until the claim is resolved, or destroy it.

Whether the information is returned or not, the producing party must preserve the information pending the court's ruling on whether the claim of privilege or of protection is properly asserted and whether it was waived. As with claims made under Rule 26(b)(5)(A), there may be no ruling if the other parties do not contest the claim.

Changes Made After Publication and Comment

The rule recommended for approval is modified from the published proposal. The rule is expanded to include trial-preparation protection claims in addition to privilege claims.

The published proposal referred to production "without intending to waive a claim of privilege." This reference to intent was deleted because many courts include intent in the factors that determine whether production waives privilege.

The published proposal required that the producing party give notice "within a reasonable time." The time requirement was deleted because it seemed to implicate the question whether production effected a waiver, a question not addressed by the rule, and also because a receiving party cannot practicably ignore a notice that it believes was unreasonably delayed. The notice procedure was further changed to require that the producing party state the basis for the claim.

Two statements in the published Note have been brought into the rule text. The first provides that the receiving party may not use or disclose the information until the claim is resolved. The second provides that if the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it.*

The rule text was expanded by adding a provision that the receiving party may promptly present the information to the court under seal for a determination of the claim.

*In response to concerns about the proposal raised at the June 15-16, 2005, Standing Committee meeting, the Committee Note was revised to emphasize that the courts will continue to examine whether a privilege claim was made at a reasonable time, as part of substantive law.

The published proposal provided that the producing party must comply with Rule 26(b)(5)(A) after making the claim. This provision was deleted as unnecessary.

Changes are made in the Committee Note to reflect the changes in the rule text.

The changes from the published rule are shown below.

* * * * *

Rule 26. General Provisions Governing Discovery; Duty of Disclosure*

* * * * *

(5) Claims of Privilege or Protection of Trial Preparation Materials.

(A) ~~***Privileged i***~~***Information Withheld.*** When 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

---

types of information may best be produced in different forms. In addition, the provision stating that a producing party need produce the same electronically stored information in only one form was relocated to make it clear that this limitation applies when the requesting party specifies the desired form or forms in the request.

The Proposed Rules and Committee Notes

Rule 33

The Committee recommends approval of the following amendment:

Rule 33. Interrogatories to Parties

* * * * *

(d) Option to Produce Business Records. Where the answer to an interrogatory may be derived or ascertained from the business records, including electronically stored information, of the party upon whom the interrogatory has been served or from an examination, audit or inspection of such business records, including a compilation, abstract or summary thereof, and the burden of deriving or ascertaining the answer is substantially the same for the party serving the interrogatory as for the party served, it is a sufficient answer to such interrogatory to specify the records from which the answer may be derived or ascertained and to afford to the party serving the interrogatory reasonable opportunity to examine, audit or inspect such records and to make copies, compilations, abstracts, or summaries. A

specification shall be in sufficient detail to permit the interrogating party to locate and to identify, as readily as can the party served, the records from which the answer may be ascertained.

* * * * *

Committee Note

Rule 33(d) is amended to parallel Rule 34(a) by recognizing the importance of electronically stored information. The term "electronically stored information" has the same broad meaning in Rule 33(d) as in Rule 34(a). Much business information is stored only in electronic form; the Rule 33(d) option should be available with respect to such records as well.

Special difficulties may arise in using electronically stored information, either due to its form or because it is dependent on a particular computer system. Rule 33(d) allows a responding party to substitute access to documents or electronically stored information for an answer only if the burden of deriving the answer will be substantially the same for either party. Rule 33(d) states that a party electing to respond to an interrogatory by providing electronically stored information must ensure that the interrogating party can locate and identify it "as readily as can the party served," and that the responding party must give the interrogating party a "reasonable opportunity to examine, audit, or inspect" the information. Depending on the circumstances, satisfying these provisions with regard to electronically stored information may require the responding party to provide some combination of technical support, information on application software, or other assistance. The key question is whether such support enables the interrogating party to derive or ascertain the answer from the electronically stored information as readily as the responding party. A party that wishes to invoke Rule 33(d) by specifying electronically stored information may be required to provide direct access to its electronic information system, but only if that is necessary to afford the requesting party an adequate opportunity to derive or ascertain the answer to the interrogatory. In that situation, the responding party's need to protect sensitive interests of confidentiality or privacy may mean that it must derive or ascertain and provide the answer itself rather than invoke Rule 33(d).

Changes Made after Publication and Comment

No changes are made to the rule text. The Committee Note is changed to reflect the sensitivities that limit direct access by a requesting party to a responding party's information system. If direct access to the responding party's system is the only way to enable a requesting party to locate and identify the records from which the answer may be ascertained, the responding party may choose to derive or ascertain the answer itself.

Rule 34

The Committee recommends the following rule amendment and accompanying Committee Note:

Rule 34. Production of Documents, Electronically Stored Information, and Things and Entry Upon Land for Inspection and Other Purposes

(a) Scope. Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, ~~and~~ copy, test, or sample any designated documents or electronically stored information — (including writings, drawings, graphs, charts, photographs, sound recordings, images ~~phonorecords~~, and other data or data compilations stored in any medium from which information can be obtained; — translated, if necessary, by the

respondent ~~through detection devices~~ into reasonably usable form~~)~~, or to inspect, ~~and~~ copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served; or (2) to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b).

(b) Procedure. The request shall set forth, either by individual item or by category, the items to be inspected, and describe each with reasonable particularity. The request shall specify a reasonable time, place, and manner of making the inspection and performing the related acts. The request may specify the form or forms in which electronically stored information is to be produced. Without leave of court or written stipulation, a request may not be served before the time specified in Rule 26(d).

The party upon whom the request is served shall serve a written response within 30 days after the service of the request. A shorter or longer time may be directed by the court or, in the absence of such an order, agreed to in writing by the parties, subject to Rule 29. The response shall state, with respect to each item or category, that inspection and related activities will be permitted as requested, unless the request is objected to, including an objection to the requested form or forms for producing electronically stored information, ~~in which event~~ stating the reasons for the objection ~~shall be stated~~. If objection is made to part of an item or category, the part shall be specified and inspection permitted of the remaining parts. 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. The party submitting the request may move for an order under Rule 37(a) with respect to any objection to or other failure to respond to the request or any part thereof, or any failure to permit inspection as requested.

Unless the parties otherwise agree, or the court otherwise orders:

(i) ~~A~~a party who produces documents for inspection shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the request;

(ii) if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable; and

(iii) a party need not produce the same electronically stored information in more than one form.

* * * * *

Committee Note

Subdivision (a). As originally adopted, Rule 34 focused on discovery of "documents" and "things." In 1970, Rule 34(a) was amended to include discovery of data compilations, anticipating that the use of computerized information would increase. Since then, the growth in electronically stored information and in the variety of systems for creating and storing such information has been dramatic. Lawyers and judges interpreted the term "documents" to include electronically stored information because it was obviously improper to allow a party to evade discovery obligations on the basis that the label had not kept pace with changes in information technology. But it has become increasingly difficult to say that all forms of electronically stored information, many dynamic in nature, fit within the traditional concept of a "document." Electronically stored information may exist in dynamic databases and other forms far different from fixed expression on paper. Rule 34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents. The change clarifies that Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined. At the same time, a Rule 34 request for production of "documents" should be understood to encompass, and the response should include, electronically stored information unless discovery in the action has clearly distinguished between electronically stored information and "documents."

Discoverable information often exists in both paper and electronic form, and the same or similar information might exist in both. The items listed in Rule 34(a) show different ways in which information may be recorded or stored. Images, for example, might be hard-copy documents or electronically stored information. The wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition of electronically stored information. Rule 34(a)(1) is expansive and includes any type of information that is stored electronically. A common example often sought in discovery is electronic communications, such as e-mail. The rule covers — either as documents or as electronically stored information — information "stored in any medium," to encompass future developments in computer technology. Rule 34(a)(1) is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments.

References elsewhere in the rules to "electronically stored information" should be understood to invoke this expansive approach. A companion change is made to Rule 33(d), making it explicit that parties choosing to respond to an interrogatory by permitting access to responsive records may do so by providing access to electronically stored information. More generally, the term used in Rule 34(a)(1) appears in a number of other amendments, such as those to Rules 26(a)(1), 26(b)(2), 26(b)(5)(B), 26(f), 34(b), 37(f), and 45. In each of these rules, electronically stored information has the same broad meaning it has under Rule 34(a)(1). References to "documents" appear in discovery

rules that are not amended, including Rules 30(f), 36(a), and 37(c)(2). These references should be interpreted to include electronically stored information as circumstances warrant.

The term "electronically stored information" is broad, but whether material that falls within this term should be produced, and in what form, are separate questions that must be addressed under Rules 26(b), 26(c), and 34(b).

The Rule 34(a) requirement that, if necessary, a party producing electronically stored information translate it into reasonably usable form does not address the issue of translating from one human language to another. *See In re Puerto Rico Elect. Power Auth.*, 687 F.2d 501, 504-510 (1st Cir. 1989).

Rule 34(a)(1) is also amended to make clear that parties may request an opportunity to test or sample materials sought under the rule in addition to inspecting and copying them. That opportunity may be important for both electronically stored information and hard-copy materials. The current rule is not clear that such testing or sampling is authorized; the amendment expressly permits it. As with any other form of discovery, issues of burden and intrusiveness raised by requests to test or sample can be addressed under Rules 26(b)(2) and 26(c). Inspection or testing of certain types of electronically stored information or of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) with regard to documents and electronically stored information 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. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems.

Rule 34(a)(1) is further amended to make clear that tangible things must — like documents and land sought to be examined — be designated in the request.

Subdivision (b). Rule 34(b) provides that a party must produce documents as they are kept in the usual course of business or must organize and label them to correspond with the categories in the discovery request. The production of electronically stored information should be subject to comparable requirements to protect against deliberate or inadvertent production in ways that raise unnecessary obstacles for the requesting party. Rule 34(b) is amended to ensure similar protection for electronically stored information.

The amendment to Rule 34(b) permits the requesting party to designate the form or forms in which it wants electronically stored information produced. The form of production is more important to the exchange of electronically stored information than of hard-copy materials, although a party might specify hard copy as the requested form. Specification of the desired form or forms may facilitate the orderly, efficient, and cost-effective discovery of electronically stored information. The rule recognizes that different forms of production may be appropriate for different types of electronically stored information. Using current technology, for example, a party might be called upon to produce word processing documents, e-mail messages, electronic spreadsheets, different image or sound files, and material from databases. Requiring that such diverse types of electronically stored information all be produced in the same form could prove impossible, and even if possible could increase the cost and burdens of producing and using the information. The rule therefore provides that the requesting party may ask for different forms of production for different types of electronically stored information.

The rule does not require that the requesting party choose a form or forms of production. The requesting party may not have a preference. In some cases, the requesting party may not know what form the producing party uses to maintain its electronically stored information, although Rule 26(f)(3) is amended to call for discussion of the form of production in the parties' prediscovery conference.

The responding party also is involved in determining the form of production. In the written response to the production request that Rule 34 requires, the responding party must state the form it intends to use for producing electronically stored information if the requesting party does not specify a form or if the responding party objects to a form that the requesting party specifies. Stating the intended form before the production occurs may permit the parties to identify and seek to resolve disputes before the expense and work of the production occurs. A party that responds to a discovery request by simply producing electronically

stored information in a form of its choice, without identifying that form in advance of the production in the response required by Rule 34(b), runs a risk that the requesting party can show that the produced form is not reasonably usable and that it is entitled to production of some or all of the information in an additional form. Additional time might be required to permit a responding party to assess the appropriate form or forms of production.

If the requesting party is not satisfied with the form stated by the responding party, or if the responding party has objected to the form specified by the requesting party, the parties must meet and confer under Rule 37(a)(2)(B) in an effort to resolve the matter before the requesting party can file a motion to compel. If they cannot agree and the court resolves the dispute, the court is not limited to the forms initially chosen by the requesting party, stated by the responding party, or specified in this rule for situations in which there is no court order or party agreement.

If the form of production is not specified by party agreement or court order, the responding party must produce electronically stored information either in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable. Rule 34(a) requires that, if necessary, a responding party "translate" information it produces into a "reasonably usable" form. Under some circumstances, the responding party may need to provide some reasonable amount of technical support, information on application software, or other reasonable assistance to enable the requesting party to use the information. The rule does not require a party to produce electronically stored information in the form it which it is ordinarily maintained, as long as it is produced in a reasonably usable form. But 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 use the information efficiently in the litigation. If 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.

Some electronically stored information may be ordinarily maintained in a form that is not reasonably usable by any party. One example is "legacy" data that can be used only by superseded systems. The questions whether a producing party should be required to convert such information to a more usable form, or should be required to produce it at all, should be addressed under Rule 26(b)(2)(B).

Whether or not the requesting party specified the form of production, Rule 34(b) provides that the same electronically stored information ordinarily need be produced in only one form.

Changes Made after Publication and Comment

The proposed amendment recommended for approval has been modified from the published version. The sequence of "documents or electronically stored information" is changed to emphasize that the parenthetical exemplifications apply equally to illustrate "documents" and "electronically stored information." The reference to "detection devices" is deleted as redundant with "translated" and as archaic.

The references to the form of production are changed in the rule and Committee Note to refer also to "forms." Different forms may be appropriate or necessary for different sources of information.

The published proposal allowed the requesting party to specify a form for production and recognized that the responding party could object to the requested form. This procedure is now amplified by directing that the responding party state the form or forms it intends to use for production if the request does not specify a form or if the responding party objects to the requested form.

The default forms of production to be used when the parties do not agree on a form and there is no court order are changed in part. As in the published proposal, one default form is "a form or forms in which [electronically stored information] is ordinarily maintained." The alternative default form, however, is changed from "an electronically searchable form" to "a form or forms that are reasonably usable." "[A]n electronically searchable form" proved to have several defects. Some electronically stored information cannot be searched electronically. In

that information became subject to a preservation obligation, the party's good faith would be measured by its efforts to arrange for the preservation of the information on that system.

The Proposed Rule and Committee Note

Rule 37(f)

The Committee recommends approval of the following proposed amendment:

Rule 37. Failure to Make Disclosures or Cooperate in Discovery; Sanctions

* * * * *

(f) Electronically stored information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

Committee Note

Subdivision (f). Subdivision (f) is new. It focuses on a distinctive feature of computer operations, the routine alteration and deletion of information that attends ordinary use. 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. As a result, the ordinary operation of computer systems creates a risk that a party may lose potentially discoverable information without culpable conduct on its part. Under Rule 37(f), absent exceptional circumstances, sanctions cannot be imposed for loss of electronically stored information resulting from the routine, good-faith operation of an electronic information system.

Rule 37(f) applies only to information lost due to the "routine operation of an electronic information system" — the ways in which such systems are generally designed, programmed, and implemented to meet the party's technical and business needs. The "routine operation" of computer systems includes the alteration and overwriting of information, often without the operator's specific direction or awareness, a feature with no direct counterpart in hard-copy documents. Such features are essential to the operation of electronic information systems.

Rule 37(f) applies to information lost due to the routine operation of an information system only if the operation was in good faith. 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 to prevent the loss of information, if that information is subject to a preservation obligation. A preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case. The good faith requirement of Rule 37(f) means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a "litigation hold." Among the factors that bear on a party's good faith in the routine operation of an information system are the steps the party took to comply with a court order in the case or party agreement requiring preservation of specific electronically stored information.

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) depends on 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.

The protection provided by Rule 37(f) applies only to sanctions "under these rules." It does not affect other sources of authority to impose sanctions or rules of professional responsibility.

This rule restricts the imposition of "sanctions." It does not prevent a court from making the kinds of adjustments frequently used in managing discovery if a party is unable to provide relevant responsive information. For example, a court could order the responding party to produce an additional witness for deposition, respond to additional interrogatories, or make similar attempts to provide substitutes or alternatives for some or all of the lost information.

Changes Made after Publication and Comment

The published rule barred sanctions only if the party who lost electronically stored information took reasonable steps to preserve the information after it knew or should have known the information was discoverable in the action. A footnote invited comment on an alternative standard that barred sanctions unless the party recklessly or intentionally failed to preserve the information. The present proposal establishes an intermediate standard, protecting against sanctions if the information was lost in the "good faith" operation of an electronic information system. The present proposal carries forward a related element that was a central part of the published proposal --- the information must have been lost in the system's "routine operation." The change to a good-faith test made it possible to eliminate the reference to information "discoverable in the action," removing a potential source of confusion as to the duty to preserve information on sources that are identified as not reasonably accessible under Rule 26(b)(2)(B).

The change to a good-faith standard is accompanied by addition of a provision that permits sanctions for loss of information in good-faith routine operation in "exceptional circumstances." This provision recognizes that in some circumstances a court should provide remedies to protect an entirely innocent party requesting discovery against serious prejudice arising from the loss of potentially important information.

As published, the rule included an express exception that denied protection if a party "violated an order in the action requiring it to preserve electronically stored information." This exception was deleted for fear that it would invite routine applications for preservation orders, and often for overbroad orders. The revised Committee Note observes

The Proposed Rule and Committee Note

Rule 45

The Committee recommends approval of amendments to Rule 45 that incorporate the corresponding changes made to the discovery rules.

Rule 45. Subpoena

(a) Form; Issuance.

(1) Every subpoena shall

(A) state the name of the court from which it is issued; and

(B) state the title of the action, the name of the court in which it is pending, and its civil action number; and

(C) command each person to whom it is directed to attend and give testimony or to produce and permit inspection, and copying, testing, or sampling of designated books, documents, electronically stored information, or tangible things in the possession, custody or control of that person, or to permit inspection of premises, at a time and place therein specified; and

(D) set forth the text of subdivisions (c) and (d) of this rule.

A command to produce evidence or to permit inspection, copying, testing, or sampling may be joined with a command to appear at trial or hearing or at deposition, or may be issued separately. A subpoena may specify the form or forms in which electronically stored information is to be produced.

(2)* A subpoena must issue as follows:

* * * * *

(C) for production, ~~and~~ inspection, copying, testing, or sampling, if separate from a subpoena commanding a person's attendance, from the court for the district where the production or inspection is to be made.

(3) The clerk shall issue a subpoena, signed but otherwise in blank, to a party requesting it, who shall complete it before service. An attorney as officer of the court may also issue and sign a subpoena on behalf of

(A) a court in which the attorney is authorized to practice; or

(B) a court for a district in which a deposition or production is compelled by the subpoena, if the deposition or production pertains to an action pending in a court in which the attorney is authorized to practice.

(b) Service.

(1) A subpoena may be served by any person who is not a party and is not less than 18 years of age. Service of a subpoena upon a person named therein shall be made by delivering a copy thereof to such person and, if the person's attendance is commanded, by tendering to that person the fees for one day's attendance and the mileage allowed by law. When the subpoena is issued on behalf of the United States or an officer or agency thereof, fees and mileage need not be tendered. Prior notice of any commanded production of documents and things or inspection of premises before trial shall be served on each party in the manner prescribed by Rule 5(b).

(2) Subject to the provisions of clause (ii) of subparagraph (c)(3)(A) of this rule, a subpoena may be served at any place within the district of the court by which it is issued, or at any

*Amendments to subdivision (a)(2) are due to take effect on December 1, 2005.

place without the district that is within 100 miles of the place of the deposition, hearing, trial, production, ~~or~~ inspection, copying, testing, or sampling specified in the subpoena or at any place within the state where a state statute or rule of court permits service of a subpoena issued by a state court of general jurisdiction sitting in the place of the deposition, hearing, trial, production, ~~or~~ inspection, copying, testing, or sampling specified in the subpoena. When a statute of the United States provides therefor, the court upon proper application and cause shown may authorize the service of a subpoena at any other place. A subpoena directed to a witness in a foreign country who is a national or resident of the United States shall issue under the circumstances and in the manner and be served as provided in Title 28, U.S.C. § 1783.

(3) Proof of service when necessary shall be made by filing with the clerk of the court by which the subpoena is issued a statement of the date and manner of service and of the names of the persons served, certified by the person who made the service.

(c) Protection of Persons Subject to Subpoenas.

(1) A party or an attorney responsible for the issuance and service of a subpoena shall take reasonable steps to avoid imposing undue burden or expense on a person subject to that subpoena. The court on behalf of which the subpoena was issued shall enforce this duty and impose upon the party or attorney in breach of this duty an appropriate sanction, which may include, but is not limited to, lost earnings and a reasonable attorney's fee.

(2) (A) A person commanded to produce and permit inspection, ~~and~~ copying, testing, or sampling of designated electronically stored information, books, papers, documents or tangible things, or inspection of premises need not appear in person at the place of production or inspection unless commanded to appear for deposition, hearing or trial.

(B) Subject to paragraph (d)(2) of this rule, a person commanded to produce and permit inspection, ~~and~~ copying, testing, or sampling may, within 14 days after service of the subpoena or before the time specified for

compliance if such time is less than 14 days after service, serve upon the party or attorney designated in the subpoena written objection to producing ~~inspection or copying of~~ any or all of the designated materials or inspection of the premises ~~or~~ to producing electronically stored information in the form or forms requested. If objection is made, the party serving the subpoena shall not be entitled to inspect, ~~and~~ copy, test, or sample the materials or inspect the premises except pursuant to an order of the court by which the subpoena was issued. If objection has been made, the party serving the subpoena may, upon notice to the person commanded to produce, move at any time for an order to compel the production, inspection, copying, testing, or sampling. Such 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, testing, or sampling commanded.

(3) (A) On timely motion, the court by which a subpoena was issued shall quash or modify the subpoena if it

(i) fails to allow reasonable time for compliance;

(ii) requires a person who is not a party or an officer of a party to travel to a place more than 100 miles from the place where that person resides, is employed or regularly transacts business in person, except that, subject to the provisions of clause (c)(3)(B)(iii) of this rule, such a person may in order to attend trial be commanded to travel from any such place within the state in which the trial is held; ~~;or~~

(iii) requires disclosure of privileged or other protected matter and no exception or waiver applies;~~;~~ or

(iv) subjects a person to undue burden.

(B) If a subpoena

(i) requires disclosure of a trade secret or other confidential research, development, or commercial information, or

(ii) requires disclosure of an unretained expert's opinion or information not describing specific events or occurrences in dispute and resulting from the expert's study made not at the request of any party, or

(iii) requires a person who is not a party or an officer of a party to incur substantial expense to travel more than 100 miles to attend trial, the court may, to protect a person subject to or affected by the subpoena, quash or modify the subpoena or, if the party in whose behalf the subpoena is issued shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship and assures that the person to whom the subpoena is addressed will be reasonably compensated, the court may order appearance or production only upon specified conditions.

(d) Duties in Responding to Subpoena.

(1) (A) A person responding to a subpoena to produce documents shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the demand.

(B) If a subpoena does not specify the form or forms for producing electronically stored information, a person responding to a subpoena must produce the information in a form or forms in which the person ordinarily maintains it or in a form or forms that are reasonably usable.

(C) A person responding to a subpoena need not produce the same electronically stored information in more than one form.

(D) A person responding to a subpoena need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or to quash, the person from whom discovery is sought must show that the information sought is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the

requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) (A) When information subject to a subpoena is withheld on a claim that it is privileged or subject to protection as trial-preparation materials, the claim shall be made expressly and shall be supported by a description of the nature of the documents, communications, or things not produced that is sufficient to enable the demanding party to contest the claim.

(B) If information is produced in response to a subpoena that is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The person who produced the information must preserve the information until the claim is resolved.

(e) Contempt. Failure ~~by~~ of any person without adequate excuse to obey a subpoena served upon that person may be deemed a contempt of the court from which the subpoena issued. An adequate cause for failure to obey exists when a subpoena purports to require a ~~non-party~~ nonparty to attend or produce at a place not within the limits provided by clause (ii) of subparagraph (c)(3)(A).

* * * * *

Committee Note

Rule 45 is amended to conform the provisions for subpoenas to changes in other discovery rules, largely related to discovery of electronically stored information. Rule 34 is amended to provide in greater detail for the production of electronically stored information. Rule 45(a)(1)(C) is amended to recognize that electronically stored information, as defined in Rule 34(a), can also be sought by subpoena. Like Rule 34(b), Rule 45(a)(1) is amended to provide that the subpoena can designate a form or forms for production of electronic data. Rule

45(c)(2) is amended, like Rule 34(b), to authorize the person served with a subpoena to object to the requested form or forms. In addition, as under Rule 34(b), Rule 45(d)(1)(B) is amended to provide that if the subpoena does not specify the form or forms for electronically stored information, the person served with the subpoena must produce electronically stored information in a form or forms in which it is usually maintained or in a form or forms that are reasonably usable. Rule 45(d)(1)(C) is added to provide that the person producing electronically stored information should not have to produce the same information in more than one form unless so ordered by the court for good cause.

As with discovery of electronically stored information from parties, complying with a subpoena for such information may impose burdens on the responding person. Rule 45(c) provides protection against undue impositions on nonparties. For example, Rule 45(c)(1) directs that a party serving a subpoena "shall take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena," and Rule 45(c)(2)(B) permits the person served with the subpoena to object to it and directs that an order requiring compliance "shall protect a person who is neither a party nor a party's officer from significant expense resulting from" compliance. Rule 45(d)(1)(D) is added to provide that the responding person need not provide discovery of electronically stored information from sources the party identifies as not reasonably accessible, unless the court orders such discovery for good cause, considering the limitations of Rule 26(b)(2)(C), on terms that protect a nonparty against significant expense. A parallel provision is added to Rule 26(b)(2).

Rule 45(a)(1)(B) is also amended, as is Rule 34(a), to provide that a subpoena is available to permit testing and sampling as well as inspection and copying. As in Rule 34, this change recognizes that on occasion the opportunity to perform testing or sampling may be important, both for documents and for electronically stored information. Because testing or sampling may present particular issues of burden or intrusion for the person served with the subpoena, however, the protective provisions of Rule 45(c) should be enforced with vigilance when such demands are made. Inspection or testing of certain types of electronically stored information or of a person's electronic information system may raise issues of confidentiality or privacy. The addition of sampling and testing to Rule 45(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a person's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems.

Rule 45(d)(2) is amended, as is Rule 26(b)(5), to add a procedure for assertion of privilege or of protection as trial-preparation materials after production. The receiving party may submit the information to the court for resolution of the privilege claim, as under Rule 26(b)(5)(B).

Other minor amendments are made to conform the rule to the changes described above.

Changes Made After Publication and Comment

The Committee recommends a modified version of the proposal as published. The changes were made to maintain the parallels between Rule 45 and the other rules that address discovery of electronically stored information. These changes are fully described in the introduction to Rule 45 and in the discussions of the other rules.

The changes from the published proposed amendment are shown below.

THE SEDONA CONFERENCE® WORKING GROUP SERIES

wgs℠

THE SEDONA GUIDELINES:
Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age

A Project of The Sedona Conference®
Working Group on
Best Practices for Electronic Document
Retention & Production

September 2005

The Sedona Conference®

THE SEDONA GUIDELINES:
Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age

Editors in Chief:
Charles R. Ragan
Jonathan M. Redgrave
Lori Ann Wagner

Senior Editors:
Christine M. Burns
David Kittrell
Judy Van Dusen

Editors:
Jacqueline M. Algon
Thomas Y. Allman
M. James Daley
James L. Michalowicz
Timothy L. Moorehead
Kate Oberlies O'Leary
Timothy M. Opsitnick
Robert F. Williams
Edward C. Wolfe

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.

wgs℠

Visit www.thesedonaconference.org

Foreword

Welcome to the second publication in The Sedona Conference® Working Group Series (the "WGS℠"). The 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 H for further information about The Sedona Conference® in general, and the WGS℠ in particular). The WGS℠ output is published and widely distributed for review, critique and comment. Following a period of peer review, we revise and republish the original piece, taking into consideration what has been learned during the comment period. The Sedona Conference® hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law and policy, both as they are and as they ought to be.

The first subject tackled by The Sedona Conference® Working Group on Best Practices for Electronic Document Retention and Production ("WG1") was electronic document production in the context of litigation. This document addresses the related and arguably larger questions related to the management of electronic information in organizations as a result of business, statutory, regulatory and legal needs. The subject of information management and record retention is of critical importance in the digital age and the subject of many treatises and publications, yet the members and participants of the Working Group believed there was a need to distill existing thoughts and, in doing so, reach across the boundaries of legal compliance, records management and information technology. The Steering Committee and participants of WG1 are to be congratulated for their efforts developing these guidelines and their continued dedication to the project since the first meeting in October of 2002. I especially want to acknowledge the contributions of Jonathan Redgrave in organizing and leading the Working Group.

The peer review period is an important part of the balanced development of these guidelines and commentary. This document was published for a six month public comment period on September 1, 2004. After the close of the comment period, the editorial board reviewed the thoughts and comments received and revised the document in light of those comments and additional legal developments since the original publication. We believe that the final work product has been improved as a result of the peer review process, and we thank every person who has contributed to this success.

Finally, while this document has now been finalized, the Working Group in the future will publish "commentaries" and other work product targeting specific issues and developments in the area of information and records management. Details of these activities will be posted on The Sedona Conference® website (www.thesedonaconference.org).

Richard G. Braman
Executive Director
The Sedona Conference®

The Sedona Guidelines for Managing Information & Records in The Electronic Age

1. An organization should have reasonable policies and procedures for managing its information and records.

a. Information and records management is important in the electronic age.
b. The hallmark of an organization's information and records management policies should be reasonableness.
c. Defensible policies need not mandate the retention of all information and documents.

2. An organization's information and records management policies and procedures should be realistic, practical and tailored to the circumstances of the organization.

a. No single standard or model can fully meet an organization's unique needs.
b. Information and records management requires practical, flexible and scalable solutions that address the differences in an organization's business needs, operations, IT infrastructure and regulatory and legal responsibilities.
c. An organization must assess its legal requirements for retention and destruction in developing an information and records management policy.
d. An organization should assess the operational and strategic value of its information and records in developing an information and records management program.
e. A business continuation or disaster recovery plan has different purposes from those of an information and records management program.

3. An organization need not retain all electronic information ever generated or received.

a. Destruction is an acceptable stage in the information life cycle; an organization may destroy or delete electronic information when there is no continuing value or need to retain it.
b. Systematic deletion of electronic information is not synonymous with evidence spoliation.
c. Absent a legal requirement to the contrary, organizations may adopt programs that routinely delete certain recorded communications, such as electronic mail, instant messaging, text messaging and voice-mail.
d. Absent a legal requirement to the contrary, organizations may recycle or destroy hardware or media that contain data retained for business continuation or disaster recovery purposes.
e. Absent a legal requirement to the contrary, organizations may systematically delete or destroy residual, shadowed or deleted data.
f. Absent a legal requirement to the contrary, organizations are not required to preserve metadata.

4. An organization adopting an information and records management policy should also develop procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.

a. Information and records management policies must be put into practice.
b. Information and records management policies and practices should be documented.
c. An organization should define roles and responsibilities for program direction and administration within its information and records management policies.
d. An organization should guide employees regarding how to identify and maintain information that has a business purpose or is required to be maintained by law or regulation.
e. An organization may choose to define separately the roles and responsibilities of content and technology custodians for electronic records management.
f. An organization should consider the impact of technology (including potential benefits) on the creation, retention and destruction of information and records.
g. An organization should recognize the importance of employee education concerning its information and records management program, policies and procedures.
h. An organization should consider conducting periodic compliance reviews of its information and records management policies and procedures, and responding to the findings of those reviews as appropriate.
i. Policies and procedures regarding electronic management and retention should be coordinated and/or integrated with the organization's policies regarding the use of property and information, including applicable privacy rights or obligations.
j. Policies and procedures should be revised as necessary in response to changes in workforce or organizational structure, business practices, legal or regulatory requirements and technology.

5. An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigation or audit.

a. An organization must recognize that suspending the normal disposition of electronic information and records may be necessary in certain circumstances.
b. An organization's information and records management program should anticipate circumstances that will trigger the suspension of normal destruction procedures.
c. An organization should identify persons with authority to suspend normal destruction procedures and impose a legal hold.
d. An organization's information and records management procedures should recognize and may describe the process for suspending normal records and information destruction and identify the individuals responsible for implementing a legal hold.
e. Legal holds and procedures should be appropriately tailored to the circumstances.
f. Effectively communicating notice of a legal hold should be an essential component of an organization's information and records management program.
g. Documenting the steps taken to implement a legal hold may be beneficial.
h. If an organization takes reasonable steps to implement a legal hold, it should not be held responsible for the acts of an individual acting outside the scope of authority and/or in a manner inconsistent with the legal hold notice.
i. Legal holds are exceptions to ordinary retention practices and when the exigency underlying the hold no longer exists (*i.e.*, there is no continuing duty to preserve the information), organizations are free to lift the legal hold.

Preface

Today most information created and received in organizations of all sizes is generated electronically in the form of e-mail messages and their attachments, word processing or spreadsheet documents, webpages, databases and the like.[1] Even formal documents—such as tax returns, applications for permits and other documents filed with regulatory authorities—generally originate, and may even be filed, in electronic format. Much of the information is never reduced to paper. Meanwhile, because of how computers operate, vast amounts of electronic data are created and maintained—seemingly forever—often without users even knowing that the data has been created, much less saved. Yet while this data is kept "seemingly forever," due to changes in technology it may rapidly become inaccessible unless migrated to new formats.[2]

This document explores how the prevalence of electronic information affects traditional concepts of records management and applicable legal requirements. It suggests basic guidelines, commentary and illustrations to help organizations develop sound and defensible processes to manage electronic information and records. The guidelines do not specify precise technical means to implement these approaches. Appropriate technical solutions can be devised only after the essential elements of a program are designed, and after reviewing the organization's operations, risk and regulatory environment and information technology (IT) structure. In all likelihood after such analysis, the application of the guidelines and the particular solutions employed will vary greatly among and even within organizations.

We examine electronic information and records management from three different perspectives—legal, records management and information technology—with legal considerations being our primary focus. In doing so, we recognize that obligations of the litigation process—such as the duty to preserve information that is, or may become, discoverable—differ from the operational needs as well as any other statutory, regulatory and other legal obligations which form the basis for records management. In large organizations, these three views are often represented by various (and perhaps well-funded) constituencies; in smaller ones, a single individual may perform two or even all three roles and the resources available may be limited. Regardless of an organization's size, an effective approach to electronic information and records management should consider all three perspectives and requires appropriate compromises in reaching the best possible solution for an organization.

One may view this document as a type of digital age Rosetta Stone,[3] helping translate and harmonize legal, records management and technical jargon and concepts for managing electronic information and records. But, like that ancient stone tablet, this document is not a radical or breakthrough paradigm for managing

1 *See* Peter Lyman & Hal R. Varian, *How Much Information 2003, available at* http://www.sims.berkeley.edu/research/projects/how-much-info-2003/.

2 On August 3, 2004 the National Archives and Records Administration (NARA) announced the award of design contracts for the agency's new Electronic Records Archive (ERA). *See* http://www.archives.gov/media_desk/press_releases/nr04-74.html. The system is being designed to "capture electronic information, regardless of its format, save it permanently, and make it accessible on whatever hardware or software is currently in use." *Id.* On September 8, 2005, NARA announced the winning contractor to develop the ERA system. *See* http://www.archives.gov/press/press-releases/2005. While the ERA system represents a significant development in the area of records management and retrieval sciences to address obsolescing data forms, it is not likely to be fully implemented sooner than 2011 and, even if it proves successful, it only represents an answer to the question of "how" to store electronic records over time rather than dictating "what" to retain.

3 The Rosetta Stone is a basalt slab discovered by Napoleon's soldiers in 1799 in Rosette (Raschid), Egypt. Carved in 196 B.C., it contains a decree of the priests of Memphis honoring the Egyptian Pharaoh Ptolemy V, appearing in hieroglyphs (the script of official and religious texts), Demotic (the script of everyday Egyptian language), and Greek. Because the Rosetta Stone contained the same text in three different scripts, for the first time in 1822 Jean Francois Champollion was able to use it to unlock the mystery of hieroglyphics. Then with the aid of his understanding of the Coptic language (the language of the Christian descendants of the ancient Egyptians), Champollion also discovered the phonetic value of the hieroglyphs, proving they had more than symbolic meaning, but also served as a "spoken language."

information and records. The Working Group readily acknowledges that others have promulgated various standards, practices and treatises on retention issues—including those for electronic records—and we do *not* seek to recreate wheels already invented. That said, the guidelines address these issues from a unique multidisciplinary perspective that we believe will help the various constituencies within an organization better understand their obligations and each other, and help persons outside the organization understand the complex and unique issues involved in managing electronic information and records.

Board of Editors[4]

4 This effort represents the collective view of The Sedona Conference® Working Group on Best Practices for Electronic Document Retention and Production and does not necessarily reflect or represent the views of The Sedona Conference®, any one participant, member or observer, or law firm/company employing a participant, or any of their clients. A list of all participants, members and observers of the Working Group is set forth in Appendix G. A description of The Sedona Conference® and its Working Group Series is set forth in Appendix H.

The Sedona Guidelines *September 2005*

Table of Contents

wgs™

Comment 2.b. Information and records management requires practical, flexible and scalable solutions that address the differences in an organization's business needs, operations, IT infrastructure and regulatory and legal responsibilities.

Comment 2.c. An organization must assess its legal requirements for retention and destruction in developing an information and records management policy.

Comment 2.d. An organization should assess the operational and strategic value of its information and records in developing an information and records management program.

Comment 2.e. A business continuation or disaster recovery plan has different purposes from those of an information and records management program.

3. An organization need not retain all electronic information ever generated or received.

Comment 3.a. Destruction is an acceptable stage in the information life cycle; an organization may destroy or delete electronic information when there is no continuing value or need to retain it.

Comment 3.b. Systematic deletion of electronic information is not synonymous with evidence spoliation.

Comment 3.c. Absent a legal requirement to the contrary, organizations may adopt programs that routinely delete certain recorded communications, such as electronic mail, instant messaging, text messaging and voice-mail.

Comment 3.d. Absent a legal requirement to the contrary, organizations may recycle or destroy hardware or media that contain data retained for business continuation or disaster recovery purposes.

Comment 3.e. Absent a legal requirement to the contrary, organizations may systematically delete or destroy residual, shadowed or deleted data.

Comment 3.f. Absent a legal requirement to the contrary, organizations are not required to preserve metadata.

4. An organization adopting an information and records management policy should also develop procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.

Comment 4.a. Information and records management policies must be put into practice.

Comment 4.b. Information and records management policies and practices should be documented.

Comment 4.c. An organization should define roles and responsibilities for program direction and administration within its information and records management policies.

Comment 4.d. An organization should guide employees regarding how to identify and maintain information that has a business purpose or is required to be maintained by law or regulation.

The Sedona Guidelines *September 2005*

Comment 4.e. An organization may choose to define separately the roles and responsibilities of content and technology custodians for electronic records management.

Comment 4.f. An organization should consider the impact (including potential benefits) of technology on the creation, retention and destruction of information and records.

Comment 4.g. An organization should recognize the importance of employee education concerning its information and records management program, policies and procedures.

Comment 4.h. An organization should consider conducting periodic compliance reviews of its information and records management policies and procedures, and responding to the findings of those reviews as appropriate.

Comment 4.i. Policies and procedures regarding electronic management and retention should be coordinated and/or integrated with the organization's policies regarding the use of property and information, including applicable privacy rights or obligations.

Comment 4.j. Policies and procedures should be revised as necessary in response to changes in work-force or organizational structure, business practices, legal or regulatory requirements and technology.

5. An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigation or audit.

Comment 5.a. An organization must recognize that suspending the normal destruction of electronic information and records may be necessary in certain circumstances.

Comment 5.b. An organization's information and records management program should anticipate circumstances that will trigger the suspension of normal destruction procedures.

Comment 5.c. An organization should identify persons with authority to suspend normal destruction procedures and impose a legal hold.

Comment 5.d. An organization's information and records management procedures should recognize and may describe the process for suspending normal records and information destruction and identify the individuals responsible for implementing a legal hold.

Comment 5.e. Legal holds and procedures should be appropriately tailored to the circumstances.

Comment 5.f. Effectively communicating notice of a legal hold should be an essential component of an organization's information and records management program.

Comment 5.g. Documenting the steps taken to implement a legal hold may be beneficial.

Comment 5.h. If an organization takes reasonable steps to implement a legal hold, it should not be held responsible for the acts of an individual acting outside the scope of authority and/or in a manner inconsistent with the legal hold notice.

wgs™

Introduction

Management of Information and Records in a World of Electronic Documents and Data

The way society communicates, creates and stores information has undergone momentous change over the past twenty years because of the "computer revolution." And certainly, when viewed in terms of the whole of human history (or even *modern* human history), this change in the way we communicate and record information has been quite sudden. Yet, laws and policies have been very slow to adapt to the new paradigm of electronic information that involves immense volumes, high volatility and great mobility. Moreover, without appropriate guidance, individual organizations have been slow to identify management solutions to the problems associated with the undifferentiated and uncontrolled growth of transmitted and stored data.[1]

This document harmonizes the legal, policy and technical considerations that bear on and should be considered by every public and private organization in today's electronic age. In particular, this publication sets forth "guidelines" to help organizations assess their unique needs and responsibilities in managing electronic information and records. Supporting each guideline is detailed commentary and citations to case law and pertinent trade literature to assist organizations in addressing these issues.[2]

In terms of structure, these guidelines focus on two distinct situations involved in the management of electronic information and records. The first, and the bulk of the document, is comprised of guidelines that address the statutory, regulatory and other legal obligations needed to manage and retain valuable information as an ongoing business matter. *See* Guidelines 1-4. The second addresses the responsibilities triggered by actual or reasonably anticipated litigation and government investigation when all types of relevant information must be preserved, regardless of whether that information has been identified as "records." *See* Guideline 5.

1. What Is a "Guideline"?

These guidelines distill respected philosophies and doctrines advocated by various treatises, white papers and studies, as well as real world experiences of The Sedona Conference® Working Group participants. The guidelines represent a framework for organizations to (a) evaluate their policies, practices and procedures, and (b) work towards "best practices" for managing information.

Significantly, these guidelines are premised on an understanding that developing and implementing an organization's best practices should be an ongoing *process* and not simply a momentary project that produces a *document*. To that end, these guidelines are not strict "standards" and may not apply in all situations.

1 *See, e.g.*, Appendix C (Summary of Cohasset Associates 2005 Survey Results); *see also* AMA/ePolicy Institute Research *2004 Workplace E-Mail and Instant Messaging Survey Summary, available at* http://www.epolicyinstitute.com/survey/survey04.pdf (last accessed 5/19/2005).

2 In 2004, the Association of Records Managers and Administrators, Inc. (ARMA) and the American National Standards Institute (ANSI) approved *Requirements for Managing Electronic Messages as Records* (ARMA/ANSI 9 2004: Oct. 7, 2004). *See also Retention Management for Records and Information* (ANSI/ARMA 8-2005: Feb. 7, 2005); *cf.* Randolph A. Kahn and Barclay T. Blair, *Information Nation Warrior: Information and Managerial Compliance Boot Camp* (AIIM 2005); *see* Randolph A. Kahn & Barclay T. Blair, *Information Nation: Seven Keys to Information Management Compliance* (AIIM 2004); Christopher V. Cotton, *Document Retention Programs for Electronic Records: Applying a Reasonableness Standard to the Electronic Era,* 24 Iowa J. CORP. L. 417 (1999); Timothy Q. Delaney, *Email Discovery: The Duties, Danger and Expense,* 46 FED. LAW. 42 (Jan. 1999); Charles A. Lovell & Roger W. Holmes, *The Dangers of Email: The Need For Electronic Data Retention Policies,* 44 R.I.B.J. 7 (Dec. 1995).

2. "Managing"[3] Information and Records

From a traditional records management perspective,[4] information should be retained as long as it has value to an organization, or is required by law or regulation to be retained.[5] Stated simply, this means that organizations must *retain* certain information when:

- A local, state or federal law or regulation mandates continued availability and accessibility;
- Internal organizational requirements, including policies and contracts or other record-keeping requirements, mandate retention, such as records for tax purposes; or
- The information is worthy of retention because it has other value to the organization.

In addition, organizations must take steps to *preserve* certain information if it is relevant to actual or reasonably anticipated litigation, subpoenas or government investigative requests, regardless of whether it meets any of the preceding criteria or constitutes a formal "record" of the organization. If, and only if, information does not meet the above criteria requiring retention or preservation, then it may be destroyed[6] and in some cases *must* be destroyed.[7]

The legitimacy of managing information and records through document and information management policies that systematically destroy (as well as retain) information has been long recognized by lower courts and, in 2005, was acknowledged by the United States Supreme Court. In the *Arthur Andersen* decision, the Court noted that "'[d]ocument retention policies' … are common in business" and added that those policies "are created in part to keep certain information from getting into the hands of others, including the Government."[8]

3 Throughout this document we use the term "information and records management" to refer to the process by which an organization generates (or receives), retains, retrieves and destroys tangible (paper or electronic) information. This "management" may be through highly detailed policies, procedures and records retention schedules, or it may be without such detail. But whatever the terms or methods employed, there are certain benefits and risks attached to these active and passive decisions, which each organization should consider and balance in its best judgment in relation to its own circumstances.

4 The traditional concept of "managing" information and records arose from practices related to paper records and, in large part, the management of inactive paper records (*i.e.*, records that were no longer actively used in the business but retained some value or fell within a legal requirement to retain the records). Records management as a discipline evolved to include paper document generation and management, and is now faced with the challenge of adjusting to the new paradigm of electronic information and records. As noted elsewhere, this challenge is exacerbated by the fact that hardware and software systems were not-and even today largely are not-designed with consideration of records retention policies and requirements.

5 The records management profession defines the various values of information to organizations as "legal values," "fiscal values," "operational values," and/or "historical values." *See ARMA Glossary of Records and Information Management Terms* (ANSI/ARMA 10 1999: Sept. 26, 2000).

6 As set forth herein, there is legitimate debate regarding whether to describe the end (last) stage of a record's "life" as "disposal" or "destruction." There is great merit to the proposition that the broader term "disposal" is better for it encompasses many possible actions and it is not as pejorative as "destruction." This document does *not*, however, take a position on such nomenclature because the important point that must be understood is that organizations can, do and should take steps to eliminate information that need not be retained, whether that is called "destruction," "deletion," "disposal," "shredding," or the like.

7 Indeed, in a world of unforeseen access to data and data loss (*see, e.g.*, Sasha Talcott, *Bank Data Loss May Affect 60 Officials*, Boston Globe, Feb. 27, 2005, at A8 (detailing loss of backup tapes by Bank of America containing sensitive information, including Social Security numbers, for 1.2 million accounts)), there is an increasing need to ensure the secure destruction of data, such as personal and financial records, after the retention or preservation periods have expired. For example, the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") became law in December 2003. Pub. L. No. 108 159 117 Stat. 1952. Section 216 of the Act required the Federal Trade Commission ("FTC") and other federal agencies to issue regulations governing the disposal of consumer credit information. The FTC final rule became effective on June 1, 2005, and creates broad responsibilities for companies that use or handle information subject to the rule. *See* 16 C.F.R. § 682, *et seq.* Section 682.3(a) of the rule states that "[a]ny person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal." 16 C.F.R. § 682.3(a).

8 *Arthur Andersen, LLP v. United States,* 544 U.S. __, 125 S. Ct. 2129, 2135 (2005). Importantly, it must be noted that the Supreme Court's decision did not endorse the actions or policies of Arthur Andersen related to its Enron-related document destruction activities that led to the criminal indictment in the first place. Instead, the Court's holding was limited to a reversal of the conviction on the basis that the jury instruction used was impermissibly broad and failed to convey the requisite level of culpability required under the then-existing statute, which had subsequently been amended as part of the Sarbanes-Oxley Act of 2002.

The Court further emphasized that "[i]t is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances." *Arthur Andersen, LLP v. United States,* 544 U.S. __, 125 S. Ct. 2129, 2135 (2005).[9]

These basic records management concepts, including the expectation that organizations will appropriately destroy information, apply equally to all forms of information, including electronic data. The challenge confronting organizations, and the objective of these guidelines and accompanying commentary, is to fashion rules, policies and programs for managing information that are feasible, effective and defensible.

3. Understanding the Distinction Between "Information" and "Records"

A prerequisite to effective management is an understanding of what is being managed. "Information" in its broadest sense is a basic resource that organizations harness to meet their operational, legal, historical and institutional needs. Every day selected pieces of this "information" are captured as "documents" or "data," giving otherwise intangible resources tangible form and enhancing the ability to access and share them. Although "information" can refer to everything from the CEO's thoughts on next quarter's forecast (intangible) to telephone message slips (tangible), throughout this document the word "information" will be used to refer generally to *all* of an organization's tangible documents and data—in both electronic and other formats and irrespective of the classification as records.

"Records" are a special subset of "information" deemed to have some enduring value to an organization and warranting special attention concerning retention, accessibility and retrieval.[10] This declaration of value can be by operation of law and/or by specific classification by the organization. Usually, the culling process:

(a) Looks at content regardless of form (electronic or paper);

(b) Focuses on the operational activities of the organization;

(c) Involves a policy level decision by the organization as to what information has sufficient value to be designated as a "record";

(d) Establishes a process by which "records" will be identified, and set aside and maintained, such that a record can be accessed and that the authenticity of the information as a business record can be readily established; and

(e) Institutes a means by which the "non-record" and "record" information will be systematically destroyed after it is no longer of value.

9 For a more extensive analysis of the impact of the *Arthur Andersen* decision, *see* Jonathan M. Redgrave, R. Christopher Cook & Charles R. Ragan, *Looking Beyond Arthur Andersen: The Impact on Corporate Records and Information Management Policies and Practices,* The Federal Lawyer (Sept. 2005).

10 Consider, for example, the following definition of a record under the United States Code:

> "[R]ecords" includes all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.

44 U.S.C. § 3301 (2000).

This culling of records from the universe of information requires management, manifested through policies, practices and education.

The unique characteristics of electronic data (as compared with paper) present unprecedented new challenges for records and information management. For example, the sheer volume of electronic communications today (such as e-mail) makes it virtually impossible for individual employees to sift and match content with lengthy records retention schedules. This leads to dual problems. On the one hand, even though much of the stored and exchanged information has only short term business value and no "record value" (for example, broadcast announcements of company social events), it may remain within the technology systems of the organization indefinitely. On the other hand, the inability to isolate and protect information of enduring value may lead to the inadvertent loss of that information to the detriment of the organization. The problem is compounded by the reality that, as of August 2005, despite many efforts to move towards centralized data, it is estimated that eighty-five percent (85%) of corporate data resides in unstructured formats outside of databases.[11]

In addition, the proliferation of "non-traditional" records within relational databases and other enterprise-wide data applications presents challenges in terms of record ownership, fixing points in time when the data should be considered to be a record, and cost-benefit analyses on disposition of data in accordance with records schedules.

As described in the included commentary, effectively classifying, retaining and destroying electronic information and records requires a combination of technical and process management solutions adapted to the unique circumstances of the organization.

4. Existing Resources to Analyze and Guide the Management of Electronic Information and Records

Two primary sources provide guidance in assessing appropriate management of information and records: (a) statutory, regulatory and other legal principles ("the law"), and (b) professional standards.

A. Legal Principles

Legal guidance is embodied in a wide variety of statutes and regulations establishing record-keeping requirements for organizations based on their locations, business operations and activities, which typically draw no distinction between electronic and paper records.[12] In addition, the common law creates obligations to preserve *evidence* (whether designated as records or not) when actual or reasonably anticipated litigation is involved.

B. Professional Standards

Many trade and service organizations recommend that their members follow published standards and technical papers addressing records and information management issues.[13] Furthermore, within certain industries, trade practices regarding data capture and retention may become standards for all industry members.

11 Eric Auchard, "Search concepts, not keywords, IBM tells business" (Reuters Aug. 8, 2005), *available at* http://www.computerworld.com/databasetopics/businessintelligence/datawarehouse/story/0,10801,103763,00.html?SKC=datawarehouse-103763.

12 Most statutes and regulations encompass both electronic and traditional paper records in their definitions of "document" or "record." In recent years, federal, state and local regulations have given organizations considerable latitude in maintaining their records in either paper or electronic form. *See, e.g.,* Paperwork Reduction Act (44 U.S.C.A. § 3501, *et seq.*) (West 2005).

13 For example, over 80 standards, recommended practices and technical reports issued by AIIM have been approved by the American National Standards Institute (ANSI). ANSI has promulgated additional national standards including, for example, storage of magnetic and optical media for records management purposes-ANSI Standard IT9.23 1998. Similarly, ARMA International and ISO (International Organization for Standardization) are accredited international standards development organizations that issue standards and reports regarding records and information management.

Organizations issuing guidance in this area include ANSI (American National Standards Institute), AIIM (Association for Information and Image Management), ARMA International (Association of Records Managers and Administrators) and ISO (International Organization for Standardization). These organizations take different and sometimes overlapping approaches to the issue, but all agree that standards are essential to manage electronic records. However, these organizations generally do not address specific litigation-oriented evidence preservation duties, a critical consideration in the United States that we address here. *See* Guideline 5 and accompanying text.

In 2001, ISO sought an international consensus standard for records management, including electronic records, in its useful guidance document ISO Technical Report 15489-2 (*Information and Documentation--Records Management* (2001)) and its accompanying standard, ISO 15489-1.[14] The standard establishes requirements to consider an organization's regulatory environment in setting records retention and disposition policies and procedures. *See* ISO 15489-1, Clause 5. The standard recognizes that there are various methods to analyze operational functions to determine records management requirements, and the Technical Report is an explicit (but not exclusive) example. Nevertheless, despite its breadth, there is no established mechanism to certify compliance with ISO 15489-1.

In 2005, ISO issued Technical Report 18492 (*Long-Term Preservation of Electronic Document-Based Information*). This technical report establishes a general framework for strategy development that can be applied to a broad range of public and private sector electronic document-based information for the long-term preservation of usable and trustworthy electronic records.[15]

Apart from the standards and guidelines offered by standards and trade organizations,[16] many consultants, vendors and software companies offer (for a price) solutions to the complex questions involved in managing information and records in the electronic age. Most of these purported solutions are oriented to specific regulatory needs (such as in the financial services or health fields) and are so new that neutral evaluation is unavailable. Furthermore, many of the white papers and technical reports that do exist often seek to advocate the narrow approach to information management offered by the vendor/author.

There is no single standard or universal policy that can be applied as a talisman to guide future conduct or judge the wisdom of prior practices for any given organization. Instead, there is a continuum of possible models, all or many of which may allow an organization to meet its unique business and legal needs. And there are infinite combinations of these approaches that may fall within the boundaries of reasonable,

14 ISO/TR 15489-2 seeks to provide a "benchmark" for "best practice" in record systems and practices, regardless of medium or format. This standard is available for purchase from the ISO online at www.iso.ch/iso/en/prods-services/ISOstore/store.html or from the ARMA bookstore at www.arma.org/bookstore/index.cfm. Australia has incorporated ISO/TR 15489-2 in its national standard for management of all records (Australian Standard AS ISO 15489 issued in 2002 replacing its groundbreaking standard AS 4390 issued in 1996). Other countries are considering adoption of the ISO standard as well, as reported in ISO's 2003 international conference report available at as reported in ISO's 2003 international conference report available at http://www.iso.org/iso/en/commcentre evenevenets/archives/2003/armaiso15489.html. An excellent summary of this ISO 2003 international conference report is available at http://www.iso.org/iso/en/commcentre/events/archives/2003/armaiso15489.html. For an excellent summary of this ISO standard, *see* Sheila Taylor, *Benchmarking for Records Management Excellence*, MUNICIPAL WORLD (Jan. 2003), *available at* http://www.condar.ca/CONDAR%20Articles/article%2015%20RM%20Benchmarking.pdf.

15 ISO Technical Report 18492 is based on the concept that electronic information constitutes the "business memory" of daily business actions or events. Following that premise, the retention and preservation of this "business memory" would seem desirable to support current and future management decisions, satisfy customers, achieve regulatory compliance, and protect against adverse litigation. Key issues in long-term preservation of electronic document-based information that are addressed in the document include the obsolescence of hardware and software and the limited life of many digital storage media. *See also* Charles M. Dollar, *Authentic Electronic Records: Strategies for Long-Term Access* (Cohasset Associates 2002).

16 Various other current standards and guidelines known to the authors of these Guidelines are set out in Appendix B. Most of the identified standards focus on technical issues relating to the use of alternative media for storing records and not on records retention issues.

defensible and good management practices. As such, the guidelines in this document do not mandate how an organization should manage its information and records. Rather, they highlight issues to consider, as well as possible steps to implement "best practices" for that organization.

5. Potential Benefits From Effective Information and Records Management

In assessing its information and records management needs, and in deciding what resources to commit, an organization may wish to consider the following possible benefits of an effective information and records management program:

- Facilitating easier and more timely access to necessary information;
- Controlling the creation and growth of information;
- Reducing operating and storage costs;
- Improving efficiency and productivity;
- Incorporating information and records management technologies as they evolve;
- Meeting statutory and regulatory retention obligations;
- Meeting litigation presentation obligations, which may be broader and more extensive than the organization's other records management obligations;
- Protecting the integrity and availability of business critical information;
- Leveraging information capital and making better decisions; and
- Preserving corporate history and memory, including evidence to support corporate governance and compliance initiatives.

While these potential benefits are difficult to quantify precisely, the emerging consensus in the literature and anecdotal experience of Working Group members lead us to conclude that organizations that comprehensively address electronic data issues in their policies and practices are better positioned to meet their legal duties (regulatory as well as in litigation) and are also more likely to maximize the value of internal business data.[17]

17 *See* Thomas Y. Allman, *Fostering a Compliance Culture: The Role of The Sedona Guidelines*, THE INFORMATION MANAGEMENT JOURNAL (ARMA April/May 2005).

6. Potential Consequences of Inadequately Managing Information and Records in the Electronic Age

An organization may also wish to consider the possible risks of not actively managing electronic information and records, such as:

- Inability to retrieve and productively use business critical information on a daily or historic basis;
- Loss of strategic opportunities due to the inability to recognize or leverage valuable information;
- Increased costs of doing business from inefficiencies related to disparate or inaccessible data;
- Failure to comply with statutory or regulatory retention and destruction requirements;
- Reduced ability to comply with court orders and other litigation-related imperatives requiring access to existing information; and
- Inability to respond promptly to government inquiries.

The consequences of a failure will vary depending upon the circumstances, but could range from minor to catastrophic:

- Lost business;
- Lost profits;
- Regulatory fines and penalties, which have recently reached eight figure amounts;[18]
- Civil litigation consequences, such as increased litigation costs, fines,19 adverse inference instructions,[20] default judgment,[21] and civil contempt;[22]
- Vicarious liability for responsible senior management;[23] and

18 *E.g.*, Bank of America was fined $10 million in March 2004 for allegedly misleading regulators and stalling in producing evidence in an investigation of improper trading at its securities brokerage. *In the Matter of Banc of Am. Sec. LLC*, SEC Admin. Proc. File No. 3 11425, Exchange Act Release No. 34 49386, 82 SEC Docket 1264 (Mar. 10, 2004), *available at* http://www.sec.gov/litigation/admin/34-49386.htm; *see also* Press Release, AmSouth Bank Agrees to Forfeit $40 Million, U.S. Department of Justice, United States Attorney, S.D. Miss.; (Oct. 12, 2004), *available at* http://www.usdoj.gov/usao/mss/documents/pressreleases/october2004/amprsrels.htm.

19 *E.g., United States v. Philip Morris USA, Inc.,* 327 F. Supp. 2d 21, 26 (D.D.C. 2004) ($2.75 million sanction for failure of 11 employees to follow litigation hold requirements for e-mails); *SEC v. Lucent Technologies Inc.,* SEC Accounting & Auditing Enforcement Release No. 2016, 82 SEC Docket 3224 (May 17, 2004) ($25 million); *In the Matter of Banc of Am. Sec. LLC,* SEC Admin. Proc. File No. 3 11425, Exchange Act Release No. 34 49386, 82 SEC Docket 1264 (Mar. 10, 2004) ($10 million); *In re Prudential Ins. Co. of Am. Sales Practices Litig.,* 169 F.R.D. 598, 617 (D.N.J. 1997) ($1 million).

20 *Coleman (Parent) Holdings Inc. v. Morgan Stanley & Co., Inc.*, No. CA 03-5045 AI, 2005 WL 674885 (Fla. Cir. Ct. Mar. 23, 2005); *Zubulake v. UBS Warburg LLC,* No. 02 Civ. 1243, 2004 WL 1620866, at *13 (S.D.N.Y. July 20, 2004); *Linnen v. A.H. Robins Co., No.* 97 2307, 10 Mass. L. Rep. 189, 1999 WL 462015, at *11 (Mass. Super. Ct. June 16, 1999).

21 *Metro. Opera Ass'n v. Local 100, Hotel Employees & Rest. Employees Int'l Union,* 212 F.R.D. 178, 231 (S.D.N.Y. 2003).

22 *Landmark Legal Found. v. EPA,* 272 F. Supp. 2d 70, 78, 89 (D.D.C. 2003).

23 Senior management may be identified by the courts with respect to failings in an organization's handling of its records. *United States v. Koch Indus. Inc.,* 197 F.R.D. 463, 483-86 (N.D. Okla. 1998); *In re Prudential Ins. Co. of Am. Sales Practices Litig.,* 169 F.R.D. 598, 615 (D.N.J. 1997).

- Criminal liability for organizations[24] and individuals.[25]

The key management challenge is to weigh the benefits (both in terms of goals achieved and risks diminished) against the potential costs of the various approaches to managing electronic documents and records. This is often described as a "cost-benefit" or ROI (*i.e.*, return on investment) analysis. The increased scrutiny in the regulatory and litigation arenas, combined with the significant complexities of managing electronic information and records, can substantially affect ROI calculations, weighing in favor of more sophisticated management approaches.

7. Enormous Challenges and Reasonable Expectations: the Road Ahead

We submit the following conclusions that can be reasonably drawn from the foregoing:

- Organizations should consider implementing information and records management policies and practices that specifically address electronic information and records, including the retention, preservation and destruction of electronic information and records.

24 Importantly, even though Arthur Andersen may have been successful in its appeal to the United States Supreme Court (*see Arthur Andersen, LLP v. United States,* 544 U.S. __, 125 S. Ct. 2129 (2005)), that decision was limited to the reversal based on an erroneous jury instruction and interpreted a statute that has since been amended. Moreover, 18 U.S.C. Section 1519, enacted as part of the Sarbanes-Oxley Act of 2002, is broader than the statutory section at issue in *Arthur Andersen* and prohibits the knowing destruction of documents "in relation to or contemplation of" "any matter within the jurisdiction of any department or agency of the United States." *See infra* note 26. In opposing certiorari in *Arthur Andersen*, the Government contended that "[m]ost federal prosecutors will henceforth use Section 1519—which does not require proof that the defendant engaged in 'corrupt persua[sion]'—to prosecute document destruction cases." Brief for the United States in Opposition, *Arthur Andersen, LLP v. United States,* 544 U.S. ___, 125 S. Ct. 2129 (2005) (No. 04 368), 2004 WL 2825876, at *13. Accordingly, the risk of criminal liability for improper document retention and destruction practices remains a real threat even after the *Arthur Andersen* decision.

25 A significant and relatively new set of obligations (and consequences) arises from the Sarbanes-Oxley Act of 2002 (the "Act"). Though much of the Act is limited to the accounting profession, a number of the provisions could theoretically be applied to anyone altering or destroying relevant electronic data. The general provisions of the Act are as follows:

- Section 802 of the Act, codified at 18 U.S.C. § 1519, makes it illegal for any person to knowingly alter or destroy records with the intent to "impede, obstruct or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States" or in any bankruptcy case. Violation of this section is punishable by up to 20 years in prison and is also punishable by fines.
- Section 802 of the Act, codified at 18 U.S.C. § 1520(b), makes it illegal for any individual to violate any rules promulgated by the Securities and Exchange Commission ("SEC") under 18 U.S.C. § 1520(a)(2) concerning the retention of "relevant records such as workpapers, documents that form the basis of an audit or review, memoranda, correspondence, communications, other documents, and records (including electronic records) which are created, sent, or received in connection with an audit or review and contain conclusions, opinions, analyses, or financial data relating to such an audit or review." Of note, the record-keeping provisions of the act apply to domestic companies and corporations, regardless of size.
- Section 1102 of the Act amends 18 U.S.C. § 1512 to create criminal penalties against anyone who "corruptly (1) alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding; or (2) otherwise obstructs, influences, or impedes any official proceeding, or attempts to do so." Violation of this section carries a penalty of up to 20 years in prison and a fine.
- Section 802 of the Act, at 18 U.S.C. § 1520(c), provides that nothing in 18 U.S.C. § 1520 "shall be deemed to diminish or relieve any person of any other duty or obligation imposed by Federal or State law or regulation to maintain, or refrain from destroying, any document."

The SEC has made clear that the governance reforms of the Act make it "necessary for companies to ensure that their internal communications and other procedures operate so that important information flows to the appropriate collection and disclosure points in a timely manner." Certification of Disclosure in Companies' Quarterly & Annual Reports, Securities Act Release No. 33 8124, Exchange Act Release No. 34 46427, Investment Company Act Release No. 25,722, 67 Fed. Reg. 57,276, at 57,280 81 (Sept. 9, 2002) (to be codified at 17 C.F.R. pts. 228, 229, 232, 240, 249, 270 & 274). *Cf. In re Tyco Int'l Ltd. Sec. Litig.,* No. 00 MD 1335, 2000 U.S. Dist. LEXIS 11659 (D.N.H. July 27, 2000) (no special preservation order is required to put defendants on notice regarding their obligation to preserve relevant electronic data and other materials, since such an order would unnecessarily duplicate or improperly alter defendants' statutory duty to preserve relevant evidence under the Securities Litigation Reform Act of 1995, 15 U.S.C. § 78u-4).

Finally, the Act imposes sanctions on any person who deletes or destroys relevant information required to be preserved. On one hand, this provides additional incentives for individual employees to comply with corporate retention policies and non-destruct notices. On the other hand, the Act also provides a valuable tool for prosecutors seeking to build cases against senior executives by plea-bargaining with low-level employees who may effectuate orders to delete data.

- Solutions for managing electronic information and records must be flexible, reasonable and scalable (*i.e.*, able to adjust from small to large organizations) to the enterprise and its circumstances. Importantly, what is seen as reasonable must be proportionate to the organization and its purpose.

- Pragmatism must guide the scope, content, costs and anticipated results of any policy or technology solution. Even though we can create and store far more than we ever imagined possible in the past, the ability to quickly create, infinitely store and potentially retrieve does not justify legal rules or arguments requiring parties to save, retrieve and produce all that is technically possible through eternity.

- Regulatory and judicial bodies must recognize that this area is enormously complex, that the boundaries of legitimate policies adopted in good faith must be sufficiently elastic, and that an organization that makes good faith efforts in this area should not be penalized for partial performance or an imperfect implementation. The failure to store or retrieve everything (or even smaller subsets) for all time should not be perceived as hiding or destroying evidence. Indeed, the Federal Rules of Civil Procedure are predicated on substantial limits on discovery that are in place to secure the "just, speedy, and inexpensive determination of every action."[26]

We respectfully offer the following guidelines, commentary and illustrations to assist organizations in creating reasonable, effective and defensible policies for managing information and records in the electronic age.

26 Fed. R. Civ. P. 1; *see also* Fed. R. Civ. P. 26(b)(2) (providing courts with discretion to manage case for efficient and appropriately tailored discovery).

The Sedona Guidelines for Managing Information & Records In The Electronic Age

1. An organization should have reasonable policies and procedures for managing its information and records.

a. Information and records management is important in the electronic age.

b. The hallmark of an organization's information and records management policies should be reasonableness.

c. Defensible policies need not mandate the retention of all information and documents.

2. An organization's information and records management policies and procedures should be realistic, practical and tailored to the circumstances of the organization.

a. No single standard or model can fully meet an organization's unique needs.

b. Information and records management requires practical, flexible and scalable solutions that address the differences in an organization's business needs, operations, IT infrastructure and regulatory and legal responsibilities.

c. An organization must assess its legal requirements for retention and destruction in developing an information and records management policy.

d. An organization should assess the operational and strategic value of its information and records in developing an information and records management program.

e. A business continuation or disaster recovery plan has different purposes from those of an information and records management program.

3. An organization need not retain all electronic information ever generated or received.

a. Destruction is an acceptable stage in the information life cycle; an organization may destroy or delete electronic information when there is no continuing value or need to retain it.

b. Systematic deletion of electronic information is not synonymous with evidence spoliation.

c. Absent a legal requirement to the contrary, organizations may adopt programs that routinely delete certain recorded communications, such as electronic mail, instant messaging, text messaging and voice-mail.

d. Absent a legal requirement to the contrary, organizations may recycle or destroy hardware or media that contain data retained for business continuation or disaster recovery purposes.

e. Absent a legal requirement to the contrary, organizations may systematically delete or destroy residual, shadowed or deleted data.

f. Absent a legal requirement to the contrary, organizations are not required to preserve metadata.

4. An organization adopting an information and records management policy should also develop procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.

a. Information and records management policies must be put into practice.

b. Information and records management policies and practices should be documented.

c. An organization should define roles and responsibilities for program direction and administration within its information and records management policies.

d. An organization should guide employees regarding how to identify and maintain information that has a business purpose or is required to be maintained by law or regulation.

e. An organization may choose to define separately the roles and responsibilities of content and technology custodians for electronic records management.

f. An organization should consider the impact of technology (including potential benefits) on the creation, retention and destruction of information and records.

g. An organization should recognize the importance of employee education concerning its information and records management program, policies and procedures.

h. An organization should consider conducting periodic compliance reviews of its information and records management policies and procedures, and responding to the findings of those reviews as appropriate.

i. Policies and procedures regarding electronic management and retention should be coordinated and/or integrated with the organization's policies regarding the use of property and information, including applicable privacy rights or obligations.

j. Policies and procedures should be revised as necessary in response to changes in workforce or organizational structure, business practices, legal or regulatory requirements and technology.

5. An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigation or audit.

a. An organization must recognize that suspending the normal disposition of electronic information and records may be necessary in certain circumstances.

b. An organization's information and records management program should anticipate circumstances that will trigger the suspension of normal destruction procedures.

c. An organization should identify persons with authority to suspend normal destruction procedures and impose a legal hold.

d. An organization's information and records management procedures should recognize and may describe the process for suspending normal records and information destruction and identify the individuals responsible for implementing a legal hold.

e. Legal holds and procedures should be appropriately tailored to the circumstances.

f. Effectively communicating notice of a legal hold should be an essential component of an organization's information and records management program.

g. Documenting the steps taken to implement a legal hold may be beneficial.

h. If an organization takes reasonable steps to implement a legal hold, it should not be held responsible for the acts of an individual acting outside the scope of authority and/or in a manner inconsistent with the legal hold notice.

i. Legal holds are exceptions to ordinary retention practices and when the exigency underlying the hold no longer exists (*i.e.*, there is no continuing duty to preserve the information), organizations are free to lift the legal hold.

Guidelines & Comments

1. An organization should have reasonable policies and procedures for managing its information and records.

Comment 1.a.
Information and records management is important in the electronic age.

The fundamental transition to an electronic data environment in most organizations has resulted in an increased need for better information and records management controls and programs. Furthermore, pressures from regulators, investors and the legal sector placing a greater emphasis on good corporate governance practices have exacerbated the need for the development of effective policies and procedures. For example, the Sarbanes-Oxley Act includes information retention requirements for auditors (15 U.S.C.A. § 7213(a)(2)(A)(i) (Thomson West Supp. 2005)), imperatives that corporate officers certify financial statements (15 U.S.C.A. § 7241 (Thomson West Supp. 2005)), and amendments to criminal statutes on obstruction of justice for failure to preserve information relevant to government "matter[s]" (18 U.S.C.A. § 1519 (Thomson West Supp. 2005)). During 2004-2005, several institutions have had multi-million dollar penalties imposed for failing to maintain or produce information as required by regulators. High visibility trials involving alleged corporate fraud or document destruction have occurred, resulting in several convictions, imprisonments and substantial monetary penalties. Still other companies have discovered that consumer records laden with sensitive private information have been inexplicably "lost."

As a result of these several converging forces, top management in many organizations is increasingly aware that identifying and managing information and records should be a business priority. Indeed, in many organizations the subject is now recognized as a "C-level" issue—one of concern to chief executive, chief financial, chief legal and chief information or technology officers. In other organizations, creating such awareness may require a significant shift in the organization's mindset, something that often occurs when an organization has its own "life-altering event."

Elevating records management to the level of asset management and including electronic information and records assets in the matrix are first steps in promoting the program and increasing its visibility. Organizations should recognize that effectively implementing an information and records management program may require significant financial and human resources. Focusing attention and resources on information as an organizational asset, and having clear rules for retention and storage, however, can produce substantial benefits. Among these potential benefits are: quicker and more reliable retrieval to assist decision-making and compliance with regulatory requests or Sarbanes-Oxley requirements; reduction of administrative time spent searching for information among cluttered systems; reduced total operating costs; minimized risk from litigation or administrative penalties; and better preservation of institutional memory. Indeed, some organizations have created the position of chief records officer (another C-level position) in recognition of these objectives to those organizations.

In short, managing electronic and other information is not merely a clerical matter. Nor, even with currently available tools, is it something that can be mastered through technology alone. Instead, it is a core component of resource management to be nurtured and enhanced. As such, managing electronic and other information

depends an intelligent blend of people, processes and technology. The organizations that best manage and leverage information assets are likely to thrive in their respective disciplines, and success in this area demands a priority commitment from senior management to develop and support effective processes.

Comment 1.b.
The hallmark of an organization's information and records management policies should be reasonableness.

An organization's approach to retaining information and records should be reasonable under the circumstances. Usually the reasonableness of an approach (including any policy) will not be subject to external scrutiny, such as a court proceeding. When such scrutiny occurs, it is often in the litigation context of explaining why specific information and records no longer exist, *i.e.*, how they were lost or destroyed. As noted in numerous cases, an established and reasonable policy may be very important in establishing the good faith destruction of the information so that no sanctions should be imposed on an organization. *See Stevenson v. Union Pacific R.R.*, 354 F.3d 739, 747 (8th Cir. 2004) (evaluating reasonableness of destruction of corporate records before and after commencement of litigation); *Willard v. Caterpillar, Inc.*, 40 Cal. App. 4th 892, 921, 48 Cal. Rptr. 2d 607, 625 (Cal. Ct. App. 1995) ("good faith disposal pursuant to a bona fide consistent and reasonable document retention policy could justify a failure to produce document in discovery.") (citing *Carlucci v. Piper Aircraft Corp.*, 102 F.R.D. 427, 481-82 (S.D. Fla. 1984)); *Turner v. Hudson Transit Lines, Inc.,* 142 F.R.D. 68, 69 (S.D.N.Y. 1991) (destruction pursuant to a document policy evidenced negligence rather than intentional conduct, but because destruction occurred after litigation was commenced, sanctions under the facts were warranted); *Telectron, Inc. v. Overhead Door Corp.,* 116 F.R.D. 107, 123 (S.D. Fla. 1987) ("The absence of a coherent document retention policy during the pendency of this lawsuit" was cited as leading to "possibly damaging document destruction occurring in both routine and non-routine manners …." Where flagrant and willful destruction of records specifically called for in production request were destroyed.); *see also* Ian C. Ballon, *Spoliation of E-mail Evidence: Proposed Intranet Policies and a Framework for Analysis*, CYBERSPACE LAWYER (March 1999) p. 4 and n.19. Furthermore, absent evidence that an organization has actual knowledge that specific information would be material to foreseeable claims or legal requirements, its best judgment about what information to retain and for how long will generally be respected. *See Arthur Andersen, LLP v. United States,* 544 U.S. __, 125 S. Ct. 2129, 2135 (2005) ("It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.") However, as is emphasized in Guideline 5, an organization must be prepared to accommodate the often broader demands of litigation which may require suspension of plans to delete or destroy information under a retention schedule based on the end of the useful life of that document. The failure to make such accommodation may call into question the reasonableness of a policy in certain circumstances. *See, e.g., Broccoli v. EchoStar Communications Corp.,* ___ F.R.D. ___, No. Civ. AMD 03 3447, 2005 WL 1863176 (D. Md. Aug. 4, 2005).

With respect to electronic information and records, a critical issue in determining reasonableness will be the information technology in place at the time. Unlike paper records, many aspects of the distribution and content of electronic information are dictated by the information technology used. Technology has an important effect on any information and records management approach. Judging reasonableness includes considering the substantial efforts required to understand new technologies and to adopt policies governing the management of electronic information and records. Considering what is reasonable (while balancing costs and benefits) also requires recognizing that the implementation of improved electronic and information management programs may take a significant amount of time and resources to implement.

When evaluating records retention policies and practices, courts routinely examine the reasonableness of the policies and practices given the facts and circumstances surrounding the information or record at issue. *See Lewy v. Remington Arms Co.*, 836 F.2d 1104, 1112 (8th Cir. 1988) (noting that retaining appointment books for three years might be reasonable, while retaining customer complaints about product safety for three years might not be reasonable); *see also United States v. Taber Extrusions L.P.*, No. 4:00CV00255, 2001 U.S. Dist. LEXIS 24600, at *8-9 (E.D. Ark. Dec. 27, 2001). In *Taber Extrusions*, the government had destroyed documents related to government contracts under its document retention policy. In analyzing the reasonableness of the destruction of those documents under *Lewy*, the court first found that the policy of destroying the documents after six years and three months appeared reasonable on its face. The court then found there was no evidence that the government should have known that the documents would become material. *Taber Extrusions*, at *9; *compare Reingold v. Wet 'N Wild Nev., Inc.,* 944 P.2d 800, 802 (Nev. 1997) (company's policy of destroying documents before statute of limitations on potential--and foreseeable--claims expired was not reasonable).

Comment 1.c.
Defensible policies need not mandate the retention of all information and documents.

There is no general requirement that organizations must retain all information created or received in the ordinary course of business, and statutory and regulatory obligations usually specify records retention requirements based on content. Indeed, in the ordinary course of business, it is expected that organizations will delete or destroy information by choice or necessity. *See Arthur Andersen, LLP v. United States*, 544 U.S. __, 125 S. Ct. 2129, 2135 (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."); Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), and regulations promulgated thereunder, notably 16 C.F.R. § 682.2(a) (*requiring* the destruction of certain consumer information in the interest of reducing "the risk of consumer fraud and related harms, including identity theft, created by improper disposal of consumer information."). Even in the context of litigation, where preservation obligations extend to evidence (and not just "records") relevant to the proceedings, courts have routinely recognized that it is unrealistic for organizations to keep *everything*. *See, e.g., Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) ("Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic document, and every backup tape? The answer is clearly, 'no.' Such a rule would cripple large corporations, like UBS, that are almost always involved in litigation."); *Wiginton v. Ellis*, No. 02 C 6832, 2003 WL 22439865, at *4, *7 (N.D. Ill. Oct. 27, 2003) (An organization "does not have to preserve every single scrap of paper in its business"; "CBRE did not have the duty to preserve every single piece of electronic data in the entire company."); *Concord Boat Corp. v. Brunswick Corp.*, No. LR C 95 781, 1997 WL 33352759, at *4 (E.D. Ark. Aug. 29, 1997) ("[T]o hold that a corporation is under a duty to preserve all e-mail potentially relevant to any future litigation would be tantamount to holding that the corporation must preserve all e-mail. … Such a proposition is not justified.").

Beyond recognizing the fact that no retention matrix, schedule or practice can realistically describe in detail or capture *all* data and information in an organization,[1] there is also a need to understand that policies and procedures cannot possibly anticipate all circumstances. In the world of rapidly evolving technology, organizations cannot be expected to always have a policy provision or practice to address all of the applied technology and communications channels. Yet organizations should recognize that static or inflexible policies and procedures run the risk of becoming outdated and unreasonable.

1 However, organizations are well served by examining and inventorying their various sources and locations of electronic documents and information. An exemplar "survey of data" containing potential inquiries for self-examination is included as Appendix D.

2. An organization's information and records management policies and procedures should be realistic, practical and tailored to the circumstances of the organization.

Comment 2.a.
No single standard or model can fully meet an organization's unique needs.

For better or worse, the extraordinary flexibility of computer network configurations directly affects the information and records management analysis. There is no single best answer for all organizations, and the course an organization takes will often depend upon its own unique information technology architecture as well as its relative dependence on technology in its business.

The development of a reasonable approach for retaining and managing electronic information and records must rest on a full understanding of how individual business users actually use the information they need in their work. The approach to managing information and records must take variances between departments, business units and other groups into account—ideally working around the differences and tailoring solutions that best advance the organization's corporate mission while meeting basic legal responsibilities.

Factors to consider include:

- The nature of the business;
- The legal and regulatory environment surrounding the organization and particular sub-units;
- The culture of the organization;
- The distributed or centralized nature of data within the organization; and
- The business practices and procedures that have evolved independently of any information or record management approach.

There are many ways that an organization can meet its goals and responsibilities in managing information and records. Some could create a centralized function for compliance. Others may invest in substantial education programs and then delegate significant responsibilities to individual employees. Others may look to automated technology solutions for records management that search content and metadata to identify, maintain and dispose of records according to pre-defined retention periods. There is no way to judge one right and one wrong approach in the abstract—the "best practice" for any one organization could be an impractical and unwise approach for another. Indeed, this variability itself makes it difficult for the organization to benchmark its own practices against others to gauge success, although some baseline comparisons can be drawn.

Critically, outsiders who one day may have to evaluate a policy or approach (whether courts, auditors, investigators or others) must recognize the fundamental reality of such variability.

The Sedona Guidelines September 2005

Comment 2.b.
Information and records management requires practical, flexible and scalable solutions that address the differences in an organization's business needs, operations, IT infrastructure and regulatory and legal responsibilities.

An information and records management program must reflect the actual use of information within an organization. It should *not* reflect an unrealistic view of either how the Legal Department "would like things to be" or how the Information Technology Department would prefer to organize the company's information for system performance or software architecture reasons, notwithstanding practical issues. Although both perspectives are important components of the ultimate design, an information and records management program with idealized or unrealistic standards (*i.e.*, ones not reasonably tailored to the organization's actual needs and usage) probably will not be appropriate for the organization's culture and will not be effective. At the same time, the records management perspective cannot dictate results that are technically or economically infeasible, or legally impermissible or unsound.

In short, the information and records management policy should recognize and be consistent with an organization's culture, actual experience and needs, as well as pre-existing structures and policies. Ivory tower drafting of a policy that states what the organization "should" do (but perhaps cannot do or never has previously done) may be worse than no policy at all.

Decisions about what electronic information should be retained and how it should be handled involve many cutting edge technological issues and conflicting policy interests. Ideally, an organization's approach to information and records management should be discussed and developed with input from legal counsel, information technology representatives, records management representatives, and representatives from the business functions of the organization to which it will apply. One possibility for larger organizations is an oversight committee composed of representatives from the functions named. In some organizations, this list may be expanded to include internal audit, human resources and other groups. In smaller companies, the responsibilities may be delegated to a very small group or even an individual. In any event, support from senior management is also important. *See United States ex rel. Koch v. Koch Indus.*, 197 F.R.D. 488, 490-91 (N.D. Okla. 1999); *In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 F.R.D. 598, 615 (D.N.J. 1997).

There is no "one size fits all" for information and records management. In some organizations, there might be a single document on the subject. In others, the organization may have a master policy with separate procedures or processes developed and implemented by departments or regions. In some cases, an organization may focus on amending an existing policy and delegating responsibility to a traditional records management department. In another, individual units may be empowered to develop and apply reasonable procedures that focus on the information needed by that unit. *See* Comment 2.a. Although examples of successful models, including exemplary written policies, are available from various sources, an organization's approach must be tailored to its own specific needs and circumstances. Drafters should consider what is reasonably possible, given the organization's structure, culture and resources. The organization should strive to demonstrate reasonable compliance with policies instituted in good faith. And, in all cases, any approach adopted must contemplate the unique needs triggered by litigation. *See* Guideline 5.

The factors in formulating an information and records management policy and procedures are numerous and complex. Among the variables to be considered, which are discussed in these Guidelines, are:

wgs

- The scope and structure of the policy (*e.g.*, whether a uniform approach is adopted worldwide, regionally, etc., and whether it applies to the organization and its wholly-owned subsidiaries, etc.);[1]
- Roles and responsibilities for creating, implementing and revising the policy. *See* Comments 4.b and 4.d;
- The types and forms of information or records that should be retained to meet operational and legal needs, including a recognition that computers produce information that must be managed in accordance with the policy. *See* Comments 2.c and 2.d;
- How the organization will document its records retention requirements (*e.g.*, through published retention schedules or through means embedded within software applications or in business procedures or some combination thereof);
- The general record-keeping practices required to manage records from point of creation or receipt to final disposition;
- Methods for monitoring and assessing compliance with the policy. *See* Comment 4.h;
- The costs and burdens that may be imposed by various approaches and policies; and
- Procedures for suspending normal destruction, as appropriate, because of actual or reasonably anticipated litigation, an investigation or audit, *i.e.*, instituting a "legal hold" on the information and records. *See* Guideline 5; *see also* Appendix F (Definition of "Legal Hold").

Perfection should never be allowed to become the enemy of good. No policy can be drafted that will be truly omnibus—there is simply too much information in too many places to cover every possible variation of facts and circumstances. Good faith efforts to develop and implement a reasonable policy should be viewed as sufficient for most purposes.

Comment 2.c.

An organization must assess its legal requirements for retention and destruction in developing an information and records management policy.

A critical step in developing an information and records management policy is identifying the applicable legal requirements concerning the retention and destruction of information. An organization must consider the externally mandated laws and regulations that govern it (*e.g.*, IRS, SEC, DOD, Department of Labor/EEOC, EPA, etc.), as well as its duties to preserve data relevant to actual or reasonably anticipated litigation. *See, e.g., Rambus, Inc. v. Infineon Techs. AG,* 220 F.R.D. 264, 281 (E.D. Va. 2004), *subsequent determination*, 222 F.R.D. 280 (E.D. Va. 2004); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003).

The organization's research likely will result in a matrix of retention obligations similar to those that were typical in traditional hard copy retention policies. Traditionally, the matrix of time periods and classifications

1 It should be noted that the less variation in a policy between departments and locations, the easier (and less expensive) it will be to train and enforce the policy across the organization.

was documented in a records retention schedule.[2] Regardless of nomenclature, the process should be the same for electronic records as for paper records, for the content rather than the format is what matters (*i.e.*, the retention schedule is generally media neutral).[3] Importantly, with the enactment of new legislation (such as Sarbanes-Oxley) and adoption of regulations (such as those implementing the Fair and Accurate Credit Transactions Act of 2003 "FACTA")), organizations must consider processes to review periodically and update policies, procedures and programs to meet changing legal requirements. *See, e.g.*, FTC Fair Credit Reporting Act Rule, 16 C.F.R. § 682.3 (implementing Section 216 of FACTA and requiring proper disposal of consumer information so as to protect against unauthorized access).

Beyond the strict legal requirements,[4] a reasonable policy can serve the legitimate information storage, access and retention needs of the organization.[5] An information and records management policy should identify and prescribe time periods for the retention of information and records that are appropriate to an organization's needs and legal responsibilities. Such a policy serves a legitimate business purpose and is not designed to eliminate potential "smoking guns." *See Lewy v. Remington Arms Co.,* 836 F.2d 1104, 1112 (8th Cir. 1988) (part three of three-part test to evaluate the reasonableness of defendant's document retention policy is whether policy was instituted in bad faith).[6] An organization focusing on eliminating "bad" documents not only risks accusations of bad faith (or worse) but also fails to recognize the value of contextual documents to mitigate the so-called "bad" documents and potentially exonerate the organization from allegations of misconduct or wrongdoing.

> ***Illustration i.*** Beta Company recently went through a merger in which the FTC required that volumes of documents, including electronic documents, be produced for antitrust review. Beta devoted substantial resources both inside and outside the company to retrieving the documents, reviewing them for relevance and copying them for the FTC. In the process, Beta concluded that many documents it reviewed served no continuing business purpose and were not responsive to the government's inquiries. It cost an additional $100,000 to review these documents. Beta has since determined that it needs a records management and retention program (with appropriate legal holds provisions) to maintain and access records for business purposes and to dispose of the records after their useful life is over. Beta's policy will likely be viewed as legitimate because it can demonstrate that business purposes were advanced by implementing the policy (and, indeed, drove its evolution).

The consequences for ill-conceived document management policies that merely serve as vehicles to "cleanse" files in advance of anticipated litigation or investigation can be severe. Indeed, a focus on concealment and

2 Many organizations already have such retention schedules for their paper records. Often, however, the schedules have not been updated and are not specifically tailored to address or incorporate electronic records.

3 There are a number of "off the shelf" software packages that, combined with regular updates, can provide a cost effective way to identify retention statutes and regulations, provided there is a way to apply changes to the manner by which the organization manages its information and records.

4 Some organizations separately schedule those documents subject to identified legal retention requirements, from those documents that are kept for business needs. Other organizations combine the categories.

5 Reasonableness standards for traditional records management programs were previously established by *Carlucci v. Piper Aircraft Corp.,* 102 F.R.D. 472 (S.D. Fla. 1984), and *Lewy v. Remington Arms Co.,* 836 F.2d 1104 (8th Cir. 1988), and still serve as the basis for assessing good faith efforts. At the same time, organizations need to recognize that, as technology changes, information and records management policies may need to be revisited and evolve as necessary to remain reasonable under the circumstances.

6 The mere existence of a written policy will not establish that document destruction was justified. Without a sound monitoring and compliance program, a records management policy may be criticized as eliminating only "bad documents." *See Carlucci v. Piper Aircraft Corp.,* 102 F.R.D. 472, 485-86 (S.D. Fla. 1984) (finding failure to implement the document retention policy in a consistent manner to be a significant factor in finding that the destruction of certain evidence relevant to legal proceedings could not be explained or excused as compliance with the policy).

damage control, as opposed to targeted retention based on operational, legal or institutional value, may even result in criminal penalties. Sections 802 and 1102 of the Sarbanes-Oxley Act of 2002 provide for fines and/or up to 20 years' imprisonment for destroying or concealing documents or other evidence with the intent to impair their availability for use in a proceeding or with the intent to impede, obstruct or influence federal investigations or bankruptcy proceedings.

In civil litigation, records management programs that focus on eliminating "bad documents" may be criticized as illegitimate "document destruction" policies that may result in severe sanctions, including default judgment. For example, in *Rambus, Inc. v. Infineon Techs. AG*, 220 F.R.D. 264, 286 (E.D. Va. 2004), *subsequent determination*, 222 F.R.D. 280 (E.D. Va. 2004), the plaintiff was plotting patent infringement litigation at the same time as it was preparing a document retention strategy that included a "Shred Day" shortly before the lawsuit was filed during which approximately 20,000 pounds of documents and approximately two million pages were destroyed. The court ordered discovery of the lawyer's files concerning the document retention program under the crime-fraud exception to the attorney-client privilege and ultimately dismissed the case. *See* Out-Law News, *Rambus Lawsuit Against Infineon Dismissed*, Feb. 3, 2005; *see also Kozlowski v. Sears, Roebuck & Co.,* 73 F.R.D. 73, 76 (D. Mass. 1976) (holding a party cannot excuse itself from compliance with discovery rules by adopting a records management system designed to make discovery unduly difficult); *Reingold v. Wet 'N Wild Nev., Inc.,* 944 P.2d 800, 802 (Nev. 1997) (holding a one season retention policy at a water park was unreasonable as "deliberately designed to prevent production of records in any subsequent litigation"; remanding for a new trial and holding that an adverse inference instruction was appropriate under the circumstances). *Compare Arthur Andersen, LLP v. United States,* 544 U.S. __, 125 S. Ct. 2129, 2135 (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."), *rev'g*, 374 F.3d 281 (5th Cir. 2004) (affirming jury verdict finding accounting firm guilty of obstructing an official proceeding of the Securities and Exchange Commission, in violation of 18 U.S.C. Section 1512(b)(2)).

> ***Illustration ii.*** Acme Corporation's stock prices have been dropping and it suspects that in its last securities offering some corners may have been cut. It reasonably anticipates that it may be named in a class action securities lawsuit or investigated for securities fraud in the foreseeable future. It implements a records management policy focused on destroying, among other things, high level e-mail communications that will probably be the focus of discovery in the investigation. Acme's policy may be viewed with a high level of scrutiny and be considered geared toward destruction of evidence, potentially subjecting it to spoliation claims and possible criminal sanctions.

For organizations with international operations or data, determining applicable legal requirements is even more complicated. For example, the Charter of Fundamental Rights of the European Union (2000/C364/01) recognizes that each person has a right to the protection of personal data and that such data must be processed fairly, for specified purposes and on the basis of the consent of the person or some other legitimate lawful basis. *Charter of Fundamental Rights of the European Union,* art. 8, 2000 O.J. (C 364) 1, 10 (Dec. 18, 2000), *available at* http://www.europarl.eu.int/charter/pdf/text_en.pdf. This right includes the fundamental right to access personal data and to correct any mistakes in that data. The legislation protecting individuals' rights in relation to personal data is mostly contained within Directive 95/46/EC on Data Protection (the "Directive"), which seeks to harmonize the applicable national legislation for each member state. Council Direct 95/46 *on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data,* 1995 O.J. (L 281) 31 (Nov. 23, 1995). In the People's Republic of China, on the other hand, there is limited regulation on document retention in place, but it is generally understood that the civil law principle protecting the right to privacy also applies in relation to the protection of personal data. *See also* Comment 4.h.

Comment 2.d.

An organization should assess the operational and strategic value of its information and records in developing an information and records management program.

Information and records can be valuable strategic assets. Indeed, organizations invest substantial capital in generating and storing electronic information representing a wealth of institutional knowledge. The value of these assets often depends on the accessibility of the information. An effective program should reflect the value of an organization's information and records.

An organization's information and records management program will necessarily reflect judgments on how best to capture and manage records, including electronic records, which have lasting value to the organization.[7] *Cf. Pub. Citizen v. Carlin,* 184 F.3d 900, 909-10 (D.C. Cir. 1999) (finding it appropriate under federal statute to allow agencies to maintain record-keeping systems in the form most appropriate to the business of the agency, reflecting its administrative, legal, research and other values, and without regard to the prospective interests of future researchers).

> ***Illustration iii.*** A large pharmaceutical manufacturer has developed several promising new leads on anti-viral drugs, but has suffered significant turnover in its lead researchers. Because the company's information and records management program specifies that all records relating to research projects should be kept for one year past the time a product resulting from the research is brought to market or three years after the research is officially terminated, the company's newest researcher is able to review the work of her predecessors and determine what areas deserve greater study without the amount of trial and error that might otherwise be necessary.

> ***Illustration iv.*** PatentCo is involved in a dispute concerning the validity of certain patents it owns, alleging that they are being infringed by several of its competitors. In developing its processes, PatentCo's scientists kept electronic laboratory notebooks detailing each step of their research and their discovery of the process that resulted in the patented invention. PatentCo's records management policy and retention schedule require that laboratory notebooks be kept permanently so that it can recreate the inventive process if necessary. When patent litigation occurs later, PatentCo is able to show that it filed its patent application less than one year from the date of its scientist's discovery of a successful process, avoiding a claim that its patent is invalid.

The value of information will vary greatly from organization to organization, and even within an organization. How an organization chooses to capture this value may also vary accordingly. One organization may choose to concentrate its resources on capturing the value in its research or product development records while another may emphasize its sales or marketing resources. The solutions, policies, practices and training employed, as well as the technological resources invested, will reflect internal business judgments as to the best approach for that entity. This makes it impossible to develop a "generic" information and records management policy appropriate for every organization. *See* Comment 2.a. Organizations should make a conscious effort to recognize and make accessible the information necessary to meet the organization's needs and responsibilities. Conversely, information not of value may and should be discarded, *see* Guideline 3, subject, of course, to the need to preserve discoverable information needed for litigation purposes. *See* Guideline 5.

7 Appendix D to this document provides a sample assessment tool that can be used as a starting point by organizations addressing records management issues, with particular emphasis on electronic information. Of course, this form is generic and will need to be tailored to fit particular circumstances.

The Sedona Guidelines *September 2005*

In addition, organizations should understand that proper information and records management is a process and not a project. Organizations continue to evolve, as do their products and services. Accordingly, in the same way that continued vigilance regarding changes in the regulatory environment is necessary, ongoing diligence regarding business structure and conditions, as well as computer hardware and software, is critical to the long-term success of any information and records management program. *See* Comment 4.i.

Comment 2.e.
A business continuation or disaster recovery plan has different purposes from those of an information and records management program.

Business continuation or disaster recovery plans and programs, such as those employing backup systems, allow an organization to rebuild its electronic information systems and to continue operations despite a significant network failure. *Cf.* Marianne Swanson *et al.,* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, CONTINGENCY PLANNING GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS (Dep't of Commerce 2002). What must be stored in order to achieve this goal and the manner and length of storage time will generally be decided by an organization's information technology professionals (with substantive input from the other disciplines—operational, records management and legal) as the individuals who will be relied on to manage the recovery. Consideration should typically be given to making the storage time period as short as possible—only that amount of time that is truly necessary to recover from a disaster.

There is general consensus that regardless of the various capabilities of different backup systems, those systems are designed for the purpose of business continuity and should not be used as a substitute for records management. While the backup systems can provide the capability to recover data when necessary, those capabilities are fundamentally different from what is required for information and records management. Moreover, after a relatively short period of time, it is simply impractical for backup systems to retrieve efficiently or effectively specific, targeted information. Reflecting this reality, the proposed amendments to the Federal Rules of Civil Procedure working their way through the approval process as of mid-2005 adopt a general rule that information stored on traditional backup tapes would not be part of a party's first-wave document production obligations, but could be the subject of discovery in a proper case where good cause is shown. *See* Proposed Amendments to Fed. R. Civ. P. 26 promulgated by the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States (August 2004), *available at* www.uscourts.gov. Accordingly, it would be useful and reasonable to reflect this in the policies, procedures and programs by separately providing for disaster recovery systems and procedures applying to electronic information and records management.

The policy for disaster recovery for electronic information should describe:

- What constitutes a "disaster" requiring information restoration;
- What must be retrieved when there is a "disaster;"
- What will be stored for access in the event of a "disaster;"
- Who has responsibility for duplicating and managing electronic information;

8 *See, e.g.,* the concept of "vital records protection" as described in *Vital Records: Identifying, Managing and Recovering Business Critical Records* (ANSI/ARMA 5 2003: Mar. 13, 2003).

- Where and how it will be stored;
- How often on-line (active or archived) electronic information will be duplicated to ensure retrieval and system recovery; and
- How long duplicate copies of electronic information must be kept before they are destroyed (through deletion or otherwise).

If disaster recovery storage devices and procedures are separate from the organization's systems for normally managing electronic information and records, then cycles for re-use of disaster recovery backup media should be relatively short, resulting in significant cost savings. *Cf.* Comment 5.e.

> ***Illustration v.*** Acme Corporation maintains disaster recovery backup tapes in the event of a system failure at its headquarters. One of the Vice-Presidents of Operations routinely deletes documents and e-mail messages that he later determines he needs to review again. He has instructed the IT staff at Acme to retain disaster recovery backup tapes indefinitely so they can find any documents he loses in the future, thinking that the cost is the incremental cost for additional storage tapes. The real costs to the company are far greater. They include: storing the extra backup tapes in a logical manner to allow retrieval if needed, having enough time to mount and load disaster recovery backup tapes to locate the server and file in question, and, most importantly, the labor costs involved in loading the data, restoring the system and locating the file. Due to Acme's recovery system configuration this process takes many hours. Thus, the cost of this ad hoc plan to recover a single lost document can quickly run into thousands of dollars, making such a program inefficient and ill-advised. Moreover, this practice may increase the risk that a court may determine the organization's backup tapes are "accessible" and hence should be part of the organization's initial response to routine discovery requests. *See Zubulake v. UBS Warburg LLC,* 217 F.R.D. 309, 324 (S.D.N.Y. 2003) (ordering production of e-mails stored on backup tapes).

The use of backup data for near-term recovery of deleted, corrupted or otherwise damaged files should not alter the consideration of disaster recovery data as an inappropriate substitute for a retention program. In particular, larger organizations today often use enterprise backup systems that maintain sophisticated database structures permitting specific files on the system to be identified and recovered with relative ease in the short term. This functionality can be very important for business purposes when an employee accidentally deletes or ruins a file that embodies significant work, or where the file becomes corrupt or damaged, or when a natural disaster (*e.g.*, flood) destroys a system. Most IT departments look at the ability to assist the business in this way as a key feature of a good backup system. Yet, the ability of the system to recover files is typically limited to a very short time period because tracking the files requires a database that soon would grow to unmanageable proportions if retention were extended. Thus, systems that address these business continuity concerns are not substitutes for records management policies and procedures which address different and longer retention concerns.

Having a meaningful policy and procedures for disaster recovery does not require that the related systems and technology must be separate from other information technology solutions for the enterprise. However, any combination must be done consciously, recognizing that the electronic information systems may be serving multiple functions.

wgs

3. An organization need not retain all electronic information ever generated or received.

Comment 3.a.

Destruction[1] is an acceptable stage in the information life cycle; an organization may destroy or delete electronic information when there is no continuing value or need to retain it.

At the heart of a reasonable information and records management approach is the concept of the "lifecycle" of information based on its inherent value. In essence, this means that information and records should be retained only so long as they have value as defined by business needs or legal requirements. Thus, while some documents contain information which is deemed irreplaceable and must be indefinitely retained, information and records that do not have such continuing value to the organization can be destroyed or deleted when the organization, in its business judgment, determines it is no longer needed, regardless of the form (*i.e.*, paper or electronic). *See Arthur Andersen, LLP v. United States,* 544 U.S. __, 125 S. Ct. 2129, 2135 (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."). Of course, this destruction in the ordinary course is subject to suspension when there is actual or reasonably anticipated litigation. *See id.*; Guideline 5 and commentary; *see also The Sedona Principles: Best Practices, Recommendations, and Principles for Addressing Electronic Document Production*, Principle No. 5 and associated commentary (Jan. 2004) ("The obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.").[2]

Retaining superfluous electronic information has associated direct and indirect costs and burdens that go well beyond the cost of additional electronic storage. The direct costs include additional disk space, bandwidth, hardware, software, archival systems and the cost of their related media migration requirements and possibly even storage area networks to store such information. The cost of storage alone can be significant, particularly where minimum standards exist concerning the storage media for such information.[3]

The indirect costs include the cost of technical staff for maintaining such information, the cost of personnel classifying such information, and the potential cost of outside counsel to review and exclude irrelevant electronic information in the discovery process.

There is no question that managing unneeded information increases an organization's costs, burdens, and ability to fashion an adequate and timely defense in litigation. For example, irrelevant electronic information can hamper efforts to locate and produce information or records that are requested in litigation. This can lead to substantial monetary sanctions when required records or information are not timely produced. *See In re Prudential Ins. Co. of Am. Sales Practices Litig.,* 169 F.R.D. 598, 615 (D.N.J. 1997) ("While there is no proof

1 We use the word "destruction" so there is no ambiguity. An organization, in drafting its policy, may use different terminology.

2 It is important to note that not all threatened litigation or conceivable disputes will trigger preservation obligations. The analysis, however, must be done on a case-by-case basis and organizations should be prepared to analyze such situations as they arise. *See* Guideline 5.

3 ANSI standards provides for storage of magnetic and digital information. *See, e.g.*, ANSI Standard IT9.23 1998 (providing guidelines for storage of polyester based magnetic tapes). These standards include monitoring of temperature and humidity levels, physical security, magnetic field restrictions, acceptable fire retardants, exercising magnetic tape to prevent stiction, etc. ("Stiction" is short for "static friction," a condition in which a hard drive's read/write heads become stuck to the disk's platters with enough strength to keep the platters from spinning, resulting in hard drive failure. *See* http://www.webopedia.com/TERM/S/stiction.html).

that Prudential, through its employees, engaged in conduct intended to thwart discovery through the purposeful destruction of documents, its haphazard and uncoordinated approach to document retention indisputably denies its party opponents potential evidence to establish facts in dispute. Because the destroyed records in Cambridge are permanently lost, the Court will draw the inference that the destroyed materials are relevant and if available would lead to the proof of a claim."). An organization can control these costs by identifying information of value to it, and reducing the amount of irrelevant electronic information that it retains. *See Smith v. Texaco, Inc.*, 951 F. Supp. 109, 112 (E.D. Tex. 1997), *settled and dismissed*, 281 F.3d 477 (5th Cir. 2002) (court upheld temporary restraining order prohibiting defendants from altering or destroying documents related to employment discrimination litigation; however, given the high cost of electronic storage, court permitted deletion of electronic documents in the ordinary course of business so long as hard copies were kept).

Managing superfluous information does not merely result in unnecessary costs. It also drains an organization's limited internal and external human and material resources. It diverts the organization's internal resources from advancing the organization's principal business objectives of efficiency and productivity. It diminishes the organization's ability to compete in the marketplace, while unduly increasing the cost of doing business. Dealing with the issues that can arise from having too much information in litigation can also divert the attention of an organization's outside counsel from strategic and substantive issues to matters of discovery and process.

Courts routinely acknowledge that organizations have the "right" to destroy (or not track or capture, whether or not it is consciously deleted) electronic information that does not meet the internal criteria of information or records requiring retention. *Arthur Andersen, LLP v. United States*, 544 U.S. __, 125 S. Ct. 2129, 2135 (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."); *see McGuire v. Acufex Microsurgical, Inc.,* 175 F.R.D. 149, 155-56 (D. Mass. 1997) (holding in the employment context, while there is no broad right to "broom clean" internal investigation files or edit personnel records "willy-nilly," employers may call for and edit drafts, and discard them where there are errors made by someone other than the accuser and noting that "[to] hold otherwise would be to create a new set of affirmative obligations for employers, unheard of in the law--to preserve all drafts of internal memos, perhaps even to record everything no matter how central to the investigation, or gratuitous"); *cf. Stevenson v. Union Pac. R.R.,* 354 F.3d 739, 748-49 (8th Cir. 2004) (recognizing legitimate aspects of a retention program that resulted in the destruction of materials relevant to the litigation). *But see Morris v. Union Pac. R.R.*, 373 F.3d 896 at 900 01 (8th Cir. 2004) (holding that adverse inference instruction sanction for destruction of engineer-dispatcher audiotape made at the time of accident was improper, distinguishing facts in *Stevenson*).

> **Illustration i.** Company A, which does not have an automated program to enforce e-mail retention and disposition, collects 1 million pages in e-mail and associated attachments from 25 employees in preparing a response to a government investigation. All pages are data converted and scanned at a cost of $0.20/page, a total of $200,000. A team of attorneys reviews the collection for relevance to the request and for privilege determinations at a cost of $0.50/page, $500,000 total. Upon completion of the culling process it is found that 10%, or 100,000 pages were responsive to the request. Company A has spent $700,000 to produce 100,000 pages. It is safe to estimate that between 50-75% of the records retained in the employee's e-mail accounts did not have "retention value." Therefore, Company A has spent between $350,000-$525,000 on processing records that had no value and were retained for no purpose.[4]

4 The figures used are hypothetical and other approaches and cost figures would yield different results.

It should be noted, however, that deciding not to track or capture electronic information does not render that information immune from discovery should litigation ensue. Accordingly, an organization may reduce the amount of superfluous electronic information that it retains even where litigation is involved, provided that its preservation obligations are met. *See* Guideline 5.

Comment 3.b.
Systematic deletion of electronic information is not synonymous with evidence spoliation.

Proper destruction of electronic records or other information consistent with a reasonable approach to managing information and records is not synonymous with spoliation of evidence or obstruction of justice. Absent extraordinary circumstances, if an organization has implemented a clearly defined records management program specifying what information and records should be kept for legal, financial, operational or knowledge value reasons and has set appropriate retention systems or periods, then information not meeting these retention guidelines can, and should, be destroyed. Destruction of this information is not spoliation of evidence. *See Willard v. Caterpillar, Inc.,* 48 Cal. Rptr. 2d 607, 625 (Cal. Ct. App. 1995) ("good faith disposal pursuant to a bona fide consistent and reasonable document retention policy could justify a failure to produce documents in discovery"), *overruled on other grounds by Cedars-Sinai Med. Ctr. v. Superior Court,* 18 Cal. 4th 1, 954 P.2d 511 (Cal. Ct. 1998); *Lewy v. Remington Arms Co.,* 836 F.2d 1104, 1112 (8th Cir. 1988) (directing the district court on remand to consider the following factors in deciding whether to instruct the jury regarding failure to produce evidence: (1) whether the records management policy is reasonable considering the facts and circumstances surrounding the relevant documents; (2) whether the policy was adopted in bad faith; and (3) whether lawsuits have been filed or complaints made in the past with such frequency or in such magnitude that it is obvious that certain categories of documents should be retained);[5] *see also Vick v. Tex. Employment Comm'n,* 514 F.2d 734, 737 (5th Cir. 1975) (affirming trial court's refusal to draw adverse inference whether documents were destroyed pursuant to Commission regulations governing disposal of inactive records); *Moore v. Gen. Motors Corp*., 558 S.W.2d 720, 735 (Mo. Ct. App. 1977) ("Anyone knowledgeable of business practices and the cost of storing records in these times would find it reasonable and not smacking of fraud for the defendant, with no knowledge of pending litigation, to follow its customary practice [of destroying records]."); *Chrysler Corp. v. Blackmon*, 841 S.W.2d 844, 847 50, 853 (Tex. 1992) (holding in products liability action, extreme sanction of default judgment was not warranted where car manufacturer failed to produce crash test reports and other documents that had been destroyed pursuant to document retention policy); *Stapper v. GMI Holdings, Inc.,* No. A091872, 2001 WL 1664920, at *9 (Cal. App. Dec. 31, 2001) (finding trial court did not abuse its discretion when it refused to allow evidence that copies of complaints made before 1995 had been destroyed pursuant to a document retention policy when there was no evidence of a willful attempt to suppress evidence and plaintiff had access to computer records with brief summaries of complaints dating to 1982).

Where an organization in good faith adopts a reasonable document retention policy, and its operation and procedures are rational, it should be permitted to continue those procedures after commencement of litigation, assuming reasonable steps have been taken to preserve data relevant to actual or reasonably anticipated litigation, government investigation or audit. *See* Martin H. Redish, *Electronic Discovery and the Litigation*

5 Some commentators argue that *Residential Funding Corp. v. DeGeorge Fin. Corp.,* 306 F.3d 99 (2nd Cir. 2002) ("RFC") creates a pure negligence standard for spoliation, which may be seen as casting doubt on the continued validity of these cases. RFC does hold that "discovery sanctions, including an adverse inference instruction, may be imposed upon a party that has breached a discovery obligation not only through bad faith or gross negligence, but also through ordinary negligence." This may be an overbroad interpretation of the importance of the RFC case, which read carefully may be significantly limited by its facts. By comparison, the case of *Stevenson v. Union Pac. R.R.*, 354 F.3d 739, 745 51 (8th Cir. 2004) makes it clear that the requirement for intentional or bad faith destruction is critical to analyzing "culpability" to determine what sanctions, if any, should attach to the loss of evidence.

Matrix, 51 DUKE L.J. 561, 621 (2001) ("(1) Electronic evidence destruction, if done routinely in the ordinary course of business, does not automatically give rise to an inference of knowledge of specific documents' destruction, much less intent to destroy those documents for litigation-related reasons, and (2) to prohibit such routine destruction could impose substantial costs and disruptive burdens on commercial enterprises."). Similar rules should apply before the formal commencement of litigation. *See generally Morris v. Union Pac.* R.R., 373 F.3d 896, 900-01 (8th Cir. 2004) (holding that adverse inference instruction sanction for destruction of engineer-dispatcher audiotape made at the time of accident was improper in circumstances of case); *Stevenson v. Union Pac. R.R.,* 354 F.3d 739, 748-49 (8th Cir. 2004) (holding adverse inference instruction was in error where records were destroyed pursuant to a document retention policy of a time when litigation was not imminent; distinguishing circumstance where pre litigation destruction of engineer-dispatcher audiotape made at time of grade crossing accident was sanctionable); *Vick v. Tex. Employment Comm'n,* 514 F.2d 734, 737 (5th Cir. 1975) (affirming trial court's refusal to draw adverse inference where documents were destroyed pursuant to Commission regulations governing disposal of inactive records); *Moore v. Gen. Motors Corp.,* 558 S.W.2d 720, 735 (Mo. Ct. App. 1977) (holding spoliation doctrine inapplicable where records were destroyed in accordance with company's customary document retention policy before litigation was anticipated); *Chrysler Corp. v. Blackmon*, 841 S.W.2d 844, 847-50, 853 (Tex. 1992) (holding sanction of default judgment not warranted where documents were destroyed pursuant to document retention policy). It is imperative, however, that destruction is carried out consistently and non selectively in conformance with the standard operating procedures for the organization.

Comment 3.c.
Absent a legal requirement to the contrary, organizations may adopt programs that routinely delete certain recorded communications, such as electronic mail, instant messaging, text messaging and voice-mail.

Unless there is an applicable retention obligation imposed by statute or regulation, or there is a legal hold imposed by virtue of litigation, audit or investigation (*see* Guideline 5), organizations can legitimately prescribe retention (or deletion) periods for recorded communications, such as electronic mail, instant messaging, voice over IP, text messaging and voice-mails. It bears emphasizing, however, that, to the extent the content communicated has value to the organization, that content—rather than the form of the communication—should dictate its management. There are several ways to approach the management of information exchanged through these communication devices. Some organizations impose space requirements (*e.g.*, 1 MB limit for e-mail boxes where users are unable to send new messages once the limit is reached). Others impose time restrictions (*e.g.*, all non-foldered e-mails more than thirty days old will be automatically deleted). Indeed, organizations can set up Instant Messaging so that archiving of the typed conversation is not allowed and the text disappears when the session is closed. Other organizations have used a hybrid approach, which provides that most communications are to be deleted within a prescribed number of days, but communications that have a true business critical nature can be retained for a longer period in public or shared folders. For example, if there is a construction project, e-mails relating to that construction project may be maintained for the life of the project in a public or shared folder, but should be deleted after the conclusion of the project.

As noted earlier, the selection of any particular solution involves complex and competing policy issues best resolved by careful discussions among an interdisciplinary team. For example, while the information technology department may effectively advocate a policy against using a network for individual archiving, employees can often archive messages on their own local hard drives (*e.g.,* with .pst files for e-mail within a Microsoft Outlook environment). This ad hoc "work around" will result in additional time and cost if the scattered information needs to be retrieved or reproduced. Organizations that rely heavily on e-mail may find

it difficult to implement a strict disposal period without sufficient safeguards to protect against the loss of important information. This highlights how important it is for organizations to adopt policies, procedures and processes that best meet their business needs, while satisfying their legal obligations.

In addition, there may be some circumstances where an organization is legally obligated to retain all forms of communications. For example, the investment industry is under a requirement to maintain for a specified period all communications with certain investment customers. *See* 17 C.F.R. § 240.17a-4(b) and (4). Alternatively, some organizations actually use e-mail to document specific transactions and, therefore, the e-mail itself might be a transactional record that should be retained under the tax laws and regulations. Before implementing a policy regarding the automatic destruction of electronic communications, the organization must have a good understanding of its legal obligations as well as its business practices.

Moreover, any organization that normally deletes data on a regular schedule should be able to suspend such automatic deletion (*i.e.*, as part of a legal hold) for some or all users, or otherwise provide a retention process or mechanism, as may be necessary to comply with preservation obligations. *See generally* John C. Montaña, *Legal Obstacles to E-Mail Message Destruction* (ARMA Int'l Educ. Found. 2003). Furthermore, organizations that adopt a time or space based approach should consider that the varying usage levels of different employees may result in the disparate application of policies and inadvertent loss of valuable information unless there is adequate education and effective procedures to cull records from non-relevant information. Indeed, a policy that routinely deletes "old" data (such as e-mail messages) without any other protections can be analogized to destroying boxes in a warehouse based on where they are on the shelf without any regard to the contents.

Organizations should also be free to migrate data from one form to another to create the record of an event or transaction. For example, many organizations have customer call centers where voice messages or customer conversations may be recorded. In the absence of a regulatory obligation, the organization, in the reasonable exercise of its business judgment, may choose to transcribe part or all of the recorded message, preserving the transcription and deleting the recording in the ordinary course. Similarly, some organizations employ unified messaging systems which convert recorded voice messages into digital formats including e-mail, and vice versa. In the absence of a regulatory obligation, the organization, in the reasonable exercise of its business judgment and consistent with a retention policy it may adopt, may choose to retain the message in only one format, or not at all.

Comment 3.d.
Absent a legal requirement to the contrary, organizations may recycle or destroy hardware or media that contain data retained for business continuation or disaster recovery purposes.

If an organization has duplicated and retained data to ensure business continuity in the event of a disaster (such as a system failure), the organization may routinely recycle that hardware or media (and destroy the temporarily retained contents) as a matter of course. *See* Comment 2.e.

The mere existence of actual or reasonably anticipated litigation, investigation or audits should not ordinarily alter such routine recycling and destruction provided that there are reasonable steps taken to preserve the relevant data maintained in other locations within the organization for such purposes. However, each organization should consider and be prepared to react to any unique circumstances that may require suspending the ordinary recycling and destruction process if it is required by court order or otherwise (*i.e.*, where the data is relevant and not being saved through some other means). *See generally* Guideline 5 and commentary.

Comment 3.e.
Absent a legal requirement to the contrary, organizations may systematically delete or destroy residual, shadowed or deleted data.

In the ordinary course of business, organizations routinely migrate information from old to new hardware and software platforms at various times. An organization need not copy and retain the residual, shadowed or deleted data[6] that may reside on the old hardware, media or system platform. Instead, as part of the migration and recycling process, such data can be routinely destroyed. In addition, organizations may routinely use processes that delete temporary data (such as residual, shadowed or deleted data) from company computers. This would include temporary files such as cached website files. Absent a specific legal or business need, there are no impediments to such destruction.

However, an organization that employs a routine system or program to destroy such data should undertake reasonable steps to identify and retain unique data that must be retained in accordance with legal obligations and also institute reasonable processes to suspend the routine destruction as may be required by court order or otherwise. *See generally* Guideline 5 and commentary.

Comment 3.f.
Absent a legal requirement to the contrary, organizations are not required to preserve metadata.

In the ordinary course of business, organizations routinely migrate information from one form to another. For example, some organizations use a printed or imaged document as the final or official version of a record. Printing an electronic document to an image (such as .tif or .pdf formats) or paper can eliminate some or all of the metadata associated with the electronic version of the document. This metadata can include system information (such as file identification tags) or it can contain potentially more meaningful information (such as author, editors, and dates associated with creation, editing or printing of the file).

Absent a specific legal or business need, an organization need not retain the electronic version of a document and its associated metadata. Indeed, the National Archives has mandated the paper retention of records in a number of instances. *Cf. Pub. Citizen v. Carlin*, 184 F.3d 900, 909-10 (D.C. Cir. 1999) (finding it appropriate under federal statute for agencies to maintain record-keeping systems in the form most appropriate to the business of the agency, reflecting its administrative, legal, research and other values, and without regard to the prospective interests of future researchers).

This is another instance where what is legally required and what an organization might do could diverge. For example, metadata may provide a wealth of information that can allow an organization to better retain and organize its information. Many organizations employ information and records management programs that specifically use metadata tags to cull and organize information. And, it may be that certain metadata is critical to an organization's ability to audit and track access to information so that it can, for example, identify and stop any improper access to sensitive information by unauthorized personnel. Thus, for some organizations it may be unworkable and unwise to routinely discard metadata. An organization should consider the best format in which to retain information to meet good business practices as well as legal requirements. *See* Comment 4.f and Appendix E.

6 See Appendix F for the definition of these terms.

Organizations should consider retaining sufficient metadata about records to ensure the trustworthiness of the records for organizational, fiscal, legal and historical purposes. If an organization migrates electronic versions with associated metadata to other versions without that metadata, the organization should consider if and how it would preserve electronic versions including metadata if it has actual notice (by court order or otherwise) that the metadata is material and needs to be preserved. For example, lawsuits may involve a need to examine the metadata associated with documents to establish facts regarding the document and its genesis, modification or distribution in particular instances. In those specific situations where particular metadata is known to be material to the dispute, the loss of such metadata may be seen as spoliation of evidence, which can have negative consequences for the organization. *See generally* Guideline 5 and commentary.

4. An organization adopting an information and records management policy should also develop procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records.

As explained earlier, an organization has considerable latitude in choosing how to manage its information and records. In this section we examine issues an organization may consider in formulating procedures to create or maintain a successful retention program. As noted earlier, there is no "one size fits all" approach to such retention programs. Organizations will take different approaches, even internally, based upon their unique history, facts and circumstances. Importantly, there must be an explicit recognition that there will be substantial differences in the approach of a 20 employee local operation versus that of a 100,000 employee multinational corporation. That said, like other aspects of corporate governance, the consistent application of the specific policies and procedures that are adopted will greatly enhance the likelihood that the program will meet its intended objectives. *See* ISO 15489-1.

Comment 4.a.
Information and records management policies must be put into practice.

The responsible handling of electronic information and records should be considered a core value of an organization. To be effective and defensible, policies should not be written and then filed on a shelf, never to be looked at again. Indeed, a policy in name only may be worse than no policy at all. Incomplete or inadequate execution of an electronic information and records management policy may result in the loss of valuable business information. For example, employees may unknowingly destroy electronic information before the end of its useful life, or store so much useless electronic information that useful information is difficult to identify or access when needed.

Comment 4.b.
Information and records management policies and practices should be documented.

An organization that has adopted a retention policy should also consider documenting its records retention efforts. The extent of the documentation will vary between organizations, and even among its several business units. A balance should be struck between making the documentation *comprehensive* and the critical need for the documentation to be *comprehended* by those tasked with executing the policies and procedures. Thus, the documentation could include an umbrella policy, procedures applicable to various departments, divisions or units, retention schedule(s), FAQ's or answers to FAQ's, copies of the training materials and resources, as well as any documents reflecting updates or changes to the policy or implementation of its provisions.

Comment 4.c.
An organization should define roles and responsibilities for program direction and administration within its information and records management policies.

Effective implementation of a reasonable information and records management policy requires the participation of individuals throughout the organization. However, some individuals necessarily have greater responsibilities in ensuring the policy's success. A clear delineation of roles and responsibilities will benefit all, and help foster the teamwork that is essential to the effort. *See* Comment 2.b.

In larger organizations prepared to invest in the process, those individuals with greater responsibilities often include:

- ***Executives and senior management***, who may oversee the creation of the information and records management policy and strategy, should provide the resources for initial and ongoing implementation and compliance, and should periodically review operational realities of the program;
- ***Records officers,*** who should (where applicable) help design and later manage the information and records policy and overall records management program;
- ***Legal department or compliance officers,*** who should be responsible for coordinating legal retention obligations, including legal holds;
- ***Business unit managers,*** who may help establish internal procedures to ensure that records of business transactions and events are created, received and retained to meet business and legal requirements; and
- ***The organization's officer or senior manager for information systems,*** who should be responsible for the reliability and continuing operation of systems used to generate, retain and dispose of electronic information and records.

Not all organizations will have the resources or personnel available or will identify a need to fill such positions. However, the manner by which an organization addresses its responsibilities is not as important as the basic identification and distribution of responsibilities so that the information and records management program can succeed in practice.

The absence of a well-coordinated multidisciplinary approach has hurt organizations in the litigation context when the preservation of data was at issue: *Coleman Holdings Inc. v. Morgan Stanley & Co., Inc.,* No. CA 03-5045 AI, 2005 WL 674885 (Fla. Cir. Ct. Mar. 23, 2005) (failure to coordinate search for backup tapes led to late discovery of more than 2,500 tapes, and partial default judgment, which contributed to jury verdict of $1.5 billion in compensatory and punitive damages); *Zubulake v. UBS Warburg LLC,* No. 02 Civ. 1243, 2004 WL 1620866, at *1, 13 (S.D.N.Y. July 20, 2004) (failure to communicate within organization and with counsel led to late productions and loss of data, warranting adverse inference instruction; jury returned $29 million verdict); *Keir v. UnumProvident Corp.,* No. 02 Civ. 8781, 2003 WL 21997747, at *6-8 (S.D.N.Y. Aug. 22, 2003) (failure to communicate order to preserve clearly, directly, timely and effectively to IT staff and outside vendor led to overwriting and loss of some electronic data); *GFTM, Inc. v. Wal Mart Stores, Inc.,* No. 98 Civ. 7724, 49 Fed. R. Serv. 3d 219, 2000 WL 335558, at *2-3 (S.D.N.Y. Mar. 30, 2000) (counsel failed to discuss the company's computer capabilities with knowledgeable person in the MIS department before representing to the court that company did not have centralized computer capability for tracking locally purchased goods; information existed at that time but was eliminated from the company's system in year following and before person-most-knowledgeable deposition, resulting in order that company pay expenses and legal fees); *United States v. Koch Indus., Inc.,* 197 F.R.D. 463, 482, 486 (N.D. Okla. 1998) (court permitted plaintiffs to inform jury that relevant computer tapes were destroyed, but did not permit adverse inference instruction where "[Defendant]'s uncoordinated approach to document retention … denied Plaintiffs potential evidence to establish the facts in dispute"); *see Landmark Legal Found. v. EPA*, 272 F. Supp. 2d 70, 79 (D.D.C. 2003) (at hearing on preliminary injunction, government represented that it would preserve responsive materials but, on motion for contempt following issuance of injunction, plaintiff established that EPA had failed to distribute preservation order widely enough to include IT staff responsible for preserving of e-mail

backup tapes, to several individuals at the agency who had the requested data, or to the acting administrator); *Linnen v. A.H. Robins Co*., No. 97-2307, 1999 Mass. Super. LEXIS 240, at *5-7, 25-33 (June 16, 1999) (where counsel for responding party did not understand client's systems for maintaining e-mail, including backup tapes, and consequently provided erroneous information to opposing counsel and the court for more than 18 months, substantial monetary sanctions were inappropriate; however, because poor communications resulted in recycling of certain backup tapes, adverse inference instruction was appropriate).

Special attention should be given to identifying an individual with broad understanding of the process who, if necessary, may serve as the declarant or witness if the policy becomes an issue. Indeed, in light of recent proposals at the state and federal court levels, such a witness may need to be identified early in any litigation. *Cf.* U.S. Dist. Ct. Ark. L.R. 26; U.S. Dist. Ct. N.J. L.R. 26; U.S. Dist. Wyo. L.R. 26; *see* Default Standard for the Discovery of Electronic Documents, ("E-Discovery") (D. Del. 2004) (J. Robinson), *available at* www.ded.uscourts.gov/SLRmain.htm.

The policy should be visibly supported by senior management. Courts in the discovery context expect that management within organizations will attend to document retention issues in a meaningful fashion. *See Danis v. USN Communications, Inc.,* No. 98 C 7482, 2000 WL 1694325, at *40-41, 53 (N.D. Ill. Oct. 23, 2000) (failure to take reasonable steps to preserve data at the outset of discovery resulted in a personal fine levied against the defendant's CEO); *In re Prudential Ins. Co. of Am. Sales Practice Litig.,* 169 F.R.D. 598, 615 (D.N.J. 1997) ("The obligation to preserve documents that are potentially discoverable materials is an affirmative one that rests squarely on the shoulders of senior corporate officers."); *see also* Daniel L. Pelc and Jonathan M. Redgrave, *Challenges for Corporate Counsel in the Land of E-Discovery: Lessons from a Case Study,* 3 ANDREWS E-BUSINESS LAW BULLETIN 1 (Feb. 2002). In determining the reasonableness of a retention policy, courts may also look to the level of support from senior management.

Comment 4.d.

An organization should guide employees regarding how to identify and maintain information that has a business purpose or is required to be maintained by law or regulation.

An organization's technology and information created with that technology are not the property of the individual employee. They are assets of the organization and should be managed accordingly. The organization's policy should set forth a process used to identify what should be retained and establish parameters to be used when selecting the most appropriate media for retention.

The records management profession generally speaks in terms of an "official record" or the official version of a record. The legal profession has long used the term "original," at least with regard to evidentiary requirements. *See* FED. R. EVID. 1002 ("To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress."); *cf.* FED. R. EVID. 1003 ("A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original."). With electronic information, such distinctions may be elusive. An organization should seek to establish criteria for determining the form and version of a record that is most appropriate to meeting its business and legal needs.

An organization should also consider the issue of "draft" documents and make rational decisions concerning their retention or destruction based on articulated business needs or legal requirements. Designating one version of data or an electronic record as the authoritative or official version does not eliminate the need to

manage other versions of that electronic information which may exist as drafts or duplicates saved by the author or recipient(s). *See* Donald Skupsky, *Establishing Records Retention Periods for Electronic Records,* INFORMATION RECORDS CLEARINGHOUSE, *available at* http://www.irch.com/articles/articl09.pdf (last visited Aug. 24, 2005).[1] Draft records include working files such as preliminary drafts, notes, supporting source documents and similar materials. Retaining draft records may assist in reconstructing events, such as the negotiations of a contract or license, and for that reason may have value to the organization. If draft records are shared with outsiders, it may also be useful to retain one complete set of those drafts that were exchanged (but not all internal drafts and comments) as proof of the development of the final document.

> ***Illustration i.*** The Director of Global Research for a company is engaged in biotechnology licensing negotiations with another company that is a direct competitor in some markets. A license is obtained and later there is a dispute about the scope of its terms. The Director is certain that a key term to support his company's position was inserted by a member of the opposing negotiation team. Others from his own team have left the company or have no memory of the exact negotiations. With the help of his lawyers he is able to reconstruct the drafting history from the set of exchanged drafts retained by the legal department.

However, absent a specific legal requirement, in most circumstances drafts of policies, memos, reports and the like will not have continuing value to the organization and need not be retained once a final record has been created. For example, draft employee evaluations could conceivably contain unique information and mental impressions concerning a decision or action, yet some courts recognize they need not be retained. *See, e.g., McGuire v. Acufex Microsurgical, Inc.,* 175 F.R.D. 149, 153-56 (D. Mass. 1997) (no obligation to preserve all drafts of internal memos and no sanctionable conduct in deleting a paragraph from a personnel evaluation even after state discrimination commission proceedings commenced; court found that employer had obligation to make sure that no false information was placed into personnel file; employer could review drafts of personnel memoranda and discard them with the editing related to obvious errors made by someone other than the accused harasser). On the other hand, drafts must be retained if they are relevant to actual or reasonably anticipated litigation, government investigation, or audit. *Trigon Ins. Co. v. United States,* 204 F.R.D. 277, 288-91 (E.D. Va. 2001) (breach of duty to preserve drafts of expert reports warrants sanctions). In such instance a legal hold should be issued to specify the need to retain records that could otherwise be discarded.

In short, an organization should consider procedures by which it captures versions of the information or record that have a separate business need for retention (*e.g.*, meaningful drafts, etc.), but then presumptively discard the rest (absent some preservation requirement).

1 *See* Donald S. Skupsky, *Legal Issues in Records Retention and Disposition Programs, available at* http://www.irch.com/articles/articl05.pdf (setting forth factors, legal requirements, and guidelines to be considered in the creation of an overall records retention and disposition program, and the procedures to be followed in developing the legal requirements section of the records retention program) (last visited Aug. 24, 2005); Donald S. Skupsky, *Applying Records Retention to Electronic Records,* INFO. MGMT. J., July 1999, at 28 (reviewing special retention problems posed by electronic records and suggesting a methodology for developing and implementing electronic record-keeping systems); David O. Stephens and Roderick C. Wallace, *Electronic Records Retention: Fourteen Basic Principles*, INFO. MGMT. J., October 2000, at 38 (examining how electronic records have transformed the nature of information management and discussing the application of traditional records retention principles for visible media to electronic record-keeping environments; the article also suggests a practical methodology for developing electronic records retention schedules).

Comment 4.e.

An organization may choose to define separately the roles and responsibilities of content and technology custodians for electronic records management.

Electronic information and records management is enhanced when records have custodians throughout their existence to ensure their credibility, reliability, accessibility and ultimate disposition or destruction. Accordingly, an organization may consider defining (formally or informally) the roles and responsibilities of employees regarding electronic information and records. The identification and role of actual "custodians" will vary with the types of tasks to be done and the point in its lifecycle of the electronic information or record. A record may require several custodians throughout its lifecycle, including a "content" as well as a "technology" custodian.

Content custodians can address creation and preservation of the information, while technology custodians may be responsible for its logistical and physical care. Content custodians may include the business unit or process owners who establish and maintain procedural controls to ensure that appropriate electronic records are created, received and retained to meet business and legal requirements. Content custodians can also include the originator or recipient of an electronic record, or their successors in the business unit function, during the normal course of business activities. These individuals are responsible for authorizing the destruction of electronic information and records in accordance with approved retention policy, and any preservation obligations due to actual or reasonably anticipated litigation, government investigation or audit.

Technology custodians can ensure that the automated environment used to generate or receive electronic records: (a) maintains appropriate metadata and content infrastructure; (b) provides mechanisms to validate electronic records authenticity and ownership; (c) protects active electronic records by implementing a comprehensive disaster recovery strategy; (d) archives inactive electronic records needed to satisfy long-term operational, historical or compliance requirements; (e) preserves electronic records and information as needed to meet litigation, investigation or audit requirements; and (f) applies the disposition requirements specified in the retention policy established by the organization to those electronic records that have exceeded their approved retention periods and that are not subject to any legal holds.

An organization may determine, especially where information has been the subject of a legal hold, that content and technology custodians should share responsibility for final disposition orders. Content custodians and technology custodians can also establish procedures to transfer the ownership of electronic information and records from one business function to the next, for example, during the course of organizational changes such as reorganizations, acquisitions/divestitures and employee retirement, termination or reassignment. *See* Comment 4.j.

An organization is responsible for managing its information and records even when it uses outside contractors to create, manage, store and dispose of information and records. As a best practice, records retention policies should extend to an organization's outside contractors, consultants and other service providers, when they are used to create, manage, store or dispose of information and records. Specific record retention requirements may need to be set forth in contracts or statements of work with those third parties.

Comment 4.f.

An organization should consider the impact (including potential benefits) of technology on the creation, retention and destruction of information and records.

For many reasons, identifying, capturing and managing electronic information and records may be a more difficult task than for paper records. The volume of electronic information generated, received and at least temporarily retained as a function of technology is significantly greater than the volume of paper information previously generated. This creates challenges in identifying and managing this greater scope of electronic information.

As a best practice, organizations should consider IT functions, structure and capabilities in developing an information and records retention policy and program. Indeed, emerging technical solutions may obviate a number of previously required human steps in classifying data in some organizations. Further, an organization should consider the impact on its retention program of proposals to migrate to new technologies or applications. For example, adopting a unified messaging system that translates recorded voice messages into digitized text files that can be stored and searched just like e-mail may have significant implications for an organization's retention program. Similarly, as today's teenagers, the overwhelming majority of whom use instant messaging daily, enter the mainstream workforce, it is likely that instant messaging and other emerging technologies will have a substantial impact on information retention practices and procedures. *See* "Teens and Technology: Youth are Leading the Transition to a Fully Wired and Mobile Nation," PEW/Internet, July 27, 2005, *available at* http://www.pewinternet.org/PPF/r/162/report_display.asp.

Metadata: An organization's information and records management policy should consider whether to preserve metadata[2] for purposes of authentication, security, data integrity, search, retrieval and analysis. Much of the metadata stored by computer systems may be meaningless from the legal or records management perspective. For example, when documents are created, the system automatically generates a variety of identifying numbers and addresses that are used purely for systems purposes. In some types of records management systems, retaining excessive metadata can needlessly increase costs of storage and complexity of a records management system. Therefore, establishing standard metadata criteria (*i.e.*, what information will be preserved and in what form) can also result in substantial savings in retrieval and storage costs.

> ***Illustration ii.*** Beta Corporation does not have a formal document management system, and it has discovered that it often has difficulty locating records that are needed for reporting purposes. Beta's records management specialist has recommended the use of document profiling within its document management software. By automatically recording basic information about the document that is supplemented by the author, important records can be located much more quickly through the use of simple searches on this metadata within the document management system.

A technical discussion about metadata and various implications in the records management context may be found in the Technical Appendix to this document, Appendix E.

Electronic Archives: An organization should consider whether, and to what extent, it uses electronic archives to store data with long-term operational, legal or historical value. Electronic archives preserve and support access to digital information and records with long retention periods that are at risk from technological

2 *See* Glossary, Appendix F.

obsolescence. Ensuring access to records in an electronic archive may be a component of an organization's best practices approach to an information and records management policy. Electronic records with continuing operational, legal or historical value may be transferred from active systems to an electronic archive. If an organization does not have an archive, special care should be taken that these records and information are otherwise properly protected. A comprehensive archive may act as a repository for both electronic and non-electronic records and thus can facilitate an integrated search of all records in all formats in the event of litigation, investigation or audit.[3]

Electronic archives are covered in greater detail in the Technical Appendix, Appendix E.

Automated Tools: An organization should consider whether, and to what extent, automated tools may be useful in managing the information and records contained in its e-mail and other systems. Users of e-mail face the challenge of dealing with many incoming and outgoing e-mail messages daily, even hourly. The life cycle of such electronic information is often extended, not because of determined value or record-keeping requirements, but because of the sheer quantity of material requiring some action. Software programs exist to facilitate automated management of e-mail messages, including "janitor" programs that dispose of e-mail based on given criteria (*e.g.*, time period expiration—30, 60, 90 days after receipt—subject line content matches, etc.), "filtering" programs that screen content and/or direct messages to appropriate parties for response, and "archiving" programs that copy messages to long-term storage and provide message indexing and security functions. These tools should be viewed as reasonable information and records management protocols with two caveats. First, the routine destruction of e-mail based on date or account size alone, such as may occur with the use of janitor programs, can result in the loss of valuable information (*e.g.*, records required to meet regulatory provisions). If janitor programs are used, care should be taken to ensure that valuable e-mail messages are protected from the operation of the janitor program. Second, the tool must allow for the preservation of relevant e-mails in the case of legal holds. *See* Guideline 5, Comment 5.e.

Should an organization always automatically suspend its e-mail management program when faced with a triggering event such as litigation? If an organization has a function or procedure in place so that e-mails and associated attachments relevant to litigation or investigation are identified and segregated to preserve them (whether by means of employees segregating the information or by use of automated tools), then it should not suspend this part of its record management program, just as it would not suspend the remainder of its program for information not subject to the legal hold.

Comment 4.g.

An organization should recognize the importance of employee education concerning its information and records management program, policies and procedures.

Organizations should strive to ensure that employees understand their responsibilities for the appropriate creation, use, retention and destruction of electronic information and records. Each of these areas in the life cycle of a record is important, has both risks and opportunities, and should be addressed in a comprehensive education or training program. Different organizations may rely on different techniques and means to communicate their policies and procedures. No one method of education or training is "best" for every organization. An organization should determine the most effective method of communicating with its employees given the nature, size and culture of the organization, and recognizing that different personalities

3 *See Electronic Records Archives Concept of Operations* (CONOPS v. 4.0); National Archives and Records Administration Electronic Records Archives Program Management Office, July 27, 2004, *available at* http://www.archives.gov/era/pdf/concept-of-operations.pdf.

receive and retain information in various ways. Often, multiple "channels" of communication, including e-mail, voice-mail, computer based training, and use of company intranets can be helpful, though such multiple approaches are certainly not mandated.

> ***Illustration iii.*** Acme Company posts its records management policy on an internal website, along with a list of frequently asked questions and the names and phone numbers of persons to call with respect to different kinds of questions (*e.g.*, legal, technical, tax) about retention issues on its intranet site. The site hosts an on-line training program where an employee answers questions about the policy and its implementation and can sign a certification that the employee has read and understands the policy.
>
> ***Illustration iv.*** BasicCo employs 50 individuals in one location and has found that company-wide meetings where policy highlights are discussed and hard copies of policies are given to each employee are the most effective means of communicating important information.

An organization's training and communication about its information and records management policy and procedures should emphasize the importance of protecting the information assets of the organization and that risks and consequences exist when this responsibility is ignored.

Documentation of the organization's efforts to educate and instruct employees can support the administration and consistent application of the policy. It may also assist an organization in defending its policy in legal proceedings.

Comment 4.h.
An organization should consider conducting periodic compliance reviews of its information and records management policies and procedures, and responding to the findings of those reviews as appropriate.

When implementing a program, an organization should be clear about its expectations for individual responsibility of employees in managing information and records. Organizations should also consider performing periodic compliance reviews of their policies and procedures for managing information and records, and respond to those reviews as necessary through use of appropriate sanctions for failure to comply (*e.g.*, under-retaining, over-retaining and failing to adhere to legal hold requirements). *Cf.* ISO 15489-1 Sections 10-11 (describing possible contours of training and auditing/monitoring programs).

Monitoring compliance with the information and records management policy is not required by law, but is a matter of sound practice. An organization can enhance its prospects for a successful retention program—and reduce its risk of exposure—if it conducts periodic reviews and takes meaningful steps to improve compliance with the program.

Some organizations require employees to acknowledge in writing their understanding of, and responsibility for adhering to, the organization's policies and procedures regarding information and records management. The use of such a procedure is highly dependent upon the organization's culture and, although not necessary for a reasonable policy or practice, it may be useful in certain organizations to assist with policy compliance. In any event, the organization's policies and procedures should also specify that policy adherence will be viewed as a component of an individual's job performance and that appropriate curative steps, including sanctions, may be administered if an employee continually fails to comply.

The review of habits concerning information housekeeping during an annual review, or the process of a litigation collection, may also uncover electronic "pack rats" or the improper use of the organization's information assets. While not part of a formal review process, some channels for feedback to those responsible for monitoring and updating the company's records management program can be beneficial.

Comment 4.i.
Policies and procedures regarding electronic management and retention should be coordinated and/or integrated with the organization's policies regarding the use of property and information, including applicable privacy rights or obligations.

Most organizations have policies that deal with the proper use of facilities and equipment primarily, if not exclusively, for business purposes. Any policies and procedures addressing information and records management ideally should dovetail with such use edicts.

In addition, most organizations have policies and procedures addressing the protection of trade secrets and competitive commercial information (such as employee non-disclosure covenants). Because much of this valuable information is now stored electronically, the need for close integration of efforts is clear.

Furthermore, statutes and regulations addressing the privacy rights of individuals (such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996) have increased the burdens on organizations to ensure that covered personal data is not improperly disclosed. Again, since most of this data resides in electronic format, the advantages of relating (if not marrying) corporate policies and objectives to technical and records management solutions becomes evident.

As noted earlier, *see* Comment 2.d, the protection of personal data in the European Union ("EU") countries is an area that also requires special attention. The Charter of Fundamental Rights of the European Union (2000/C364/01) recognizes that each person has a right to the protection of personal data and that such data must be processed fairly, for specified purposes and on the basis of the consent of the person or some other legitimate lawful basis (Article 8). *Charter of Fundamental Rights of the European Union*, art. 8, 2000 O.J. (C 364) 1 (Dec. 18, 2000), *available at* http://www.europarl.eu.int/charter/pdf/text_en.pdf. This right is mostly contained within Directive 95/46/EC on Data Protection (the "Directive") and applies to any data that identifies an individual, including name, address, telephone number or specific physical characteristics. The collection, storage, retrieval, transmission and destruction of data all fall within the definition of "processing" under the Directive. The majority of the obligations with respect to personal data falls on "data controllers," defined as those responsible for processing personal data. The Directive establishes that data controllers must adhere to the following key rules:

- Personal data may only be processed as described to the data subject and with the data subject's consent, unless a specified exception applies (such as when the processing is necessary for performance of a contract to which the data subject is party).
- Data subjects must be given the opportunity to rectify, erase or prevent the use of incorrect personal data.
- Personal data must not be kept longer than is necessary under the circumstances.
- Except in certain circumstances personal data may not be exported from the European Economic Area ("EEA").

- The processing of sensitive data (race, ethnicity, political opinions, religion, trade-union membership, health or sexual preference) is subject to further restrictions, including the need for the data subject to give informed consent to the processing.

U.S. companies have been fined for providing unsatisfactory protection of personal data. For example, in 2001 Microsoft was fined approximately $60,000 by the Spanish Data Protection Agency for failing to implement sufficient controls when it transferred employee data outside of the EU. *See* http://www.privacy international.org/survey/phr2003/countries/spain.htm. As of the time of this publication, the EU has determined that generally the United States does not provide adequate protection for personal data, except for: (a) the specific provisions of the U.S. Department of Commerce's Safe Harbor Privacy Principles; and (b) the transfer of Air Passenger Name Record to the United States Bureau of Customs and Border Protection. *See* Press Release, "Commission decisions on the adequacy of the protection of personal data in third countries" *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm and attached documents, including: "Opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America (30.9.2004)" and "Commission Decision 2000/520/EC of 26.7.2000 - O. J. L 215/7 of 25.8.2000" pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal date provided by the Safe Harbour Privacy Principles. (Last accessed 08/22/2005.)

Comment 4.j.
Policies and procedures should be revised as necessary in response to changes in workforce or organizational structure, business practices, legal or regulatory requirements and technology.

The complexity of managing disparate and ever-changing electronic records is heightened by the fact that most organizations themselves are dynamic—organizations grow and shrink, businesses and assets are bought and sold, employees come and go. Policies and procedures should remain relevant and evolve with changes in legal requirements, organizational structure, business practices and technology. The information and records management policy should be periodically reviewed and revised as required to address changes in business processes that may affect the organization's information and records management practices.

From an operational and records management perspective, organizations should develop procedures to address the disposal and/or transfer of electronic information and records in such a dynamic business and technology climate. For example, when businesses sell information assets, knowing what should and should not be retained is critical. The transition program should address these data ownership issues.

A more common example is where an employee leaves a particular job function or the organization. Procedures governing what to do with electronic information and records associated with that employee will reduce risk (loss of assets) and manage costs (storage of records without owners). One possible approach (among many) is to inventory the employee's electronic records and to assign custody of them to the employee's manager. The manager can then coordinate the review, inheritance and retention of these records, as appropriate. And the manager, or delegate, can provide the appropriate direction to the information technology department concerning the migration or other disposition of the information.

From a legal perspective, there may be circumstances when the legal department should determine whether some or all of the electronic information associated with certain departing employees should be retained. In developing its policies and procedures, an organization should consider the circumstances in which the legal department's involvement is important and provide for mechanisms to incorporate it. It is important to coordinate the efforts of the human resources, law and IT departments closely in these situations, to avoid unintended consequences.

5. An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigation or audit.

Comment 5.a.

An organization must recognize that suspending the normal destruction of electronic information and records may be necessary in certain circumstances.

An organization's information and records management policy must recognize that certain events will impose a duty to preserve potential evidence or otherwise justify suspending the normal course of records destruction, including the normal procedures for disposing of electronic information and records. Circumstances that may require suspending normal destruction of electronic information and records would include, among others: actual or reasonably anticipated[1] litigation; government investigation[2] or audit; preservation orders issued in active litigation; and certain business-related scenarios (*e.g.*, mergers or acquisitions, technology reviews, bankruptcy). In the event of such circumstances, an organization must suspend its normal document retention procedures and preserve all relevant information (even if not of "record" quality). *See* Comment 5.e.

Comment 5.b.

An organization's information and records management program should anticipate circumstances that will trigger the suspension of normal destruction procedures.

Ideally, an organization's information and records management program should have an established process by which it evaluates whether a duty to preserve arises as a result of actual or reasonably anticipated litigation, government investigation or audit. Circumstances constituting such notice may include, but are not limited to: an inquiry from the government, service of a complaint or petition commencing litigation or a third-party request for documents. *See Arthur Andersen, LLP v. United States*, 544 U.S. __, 125 S. Ct. 2129, 2131-33 & n.4 (2005) (accounting firm had knowledge of likely SEC investigation of Enron-related work but did not suspend ordinary destruction practices (and actually invigorated dormant destruction practices under its retention policy) until receipt of subpoena for records; Court reversed conviction due to erroneous jury instruction, without deciding whether the accounting firm had followed its own document retention and litigation hold policy); *Stevenson v. Union Pac. R.R.,* 354 F.3d 739, 747-48 (8th Cir. 2004) (where defendant railroad was aware that accidents resulting in death or serious injury were likely to result in a lawsuit and that audio tapes were the sole source of particularly relevant evidence, appellate court upheld district court's determination that it was bad faith to destroy the tapes after learning of such an accident even prior to litigation being commenced); *Rambus, Inc. v. Infineon Techs. AG,* 220 F.R.D. 264, 286-87 (E.D. Va. 2004), *subsequent determination*, 222 F.R.D. 280 (E.D. Va. 2004) (where plaintiff knew it was likely to bring litigation it could not create program with intent to destroy relevant evidence); *Renda Marine, Inc. v. United States*, 58 Fed. Cl. 57, 61-62 (2003) (defendant put on reasonable notice of litigation, and duty to preserve triggered when dispute arose, and defendant's officer issued cure notice to plaintiff); *Applied Telematics, Inc. v. Sprint Communications Co.,* No. 94-4603, 1996 U.S. Dist. LEXIS 14053, at *6 (E.D. Pa. Sept. 17, 1996) (duty to

1 Some courts and commentators refer to "reasonably anticipated litigation" as "threatened" litigation. The terminology employed is not as important as the concept: there must be some specific set of facts and circumstances that would lead to a conclusion that litigation is imminent or should otherwise be expected. The mere fact that litigation regarding a topic (such as a product or a contract) is a general possibility is ordinarily not enough to trigger preservation obligations.

2 18 U.S.C. § 1519 was amended (as section 802 of the Sarbanes-Oxley Act, H.R. 3763) to expend criminal penalties for destroying documents with the intent to impede or obstruct a government investigation of *any matter* before a U.S. department or agency.

preserve arises when party possessing the evidence has notice of relevance; this may be triggered as soon as complaint is served, but certainly arises once discovery request has been propounded); *Lombardo v. Broadway Stores, Inc.,* No. G026581, 2002 WL 86810, at *9-10 (Cal. Ct. App. 4 Dist. Jan. 22, 2002) (breach of duty to preserve occurred when defendant permitted destruction of electronic evidence after commencement of class action suit and plaintiff had twice requested that defendant preserve relevant data in the months prior to litigation); *cf. Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216-17 (S.D.N.Y. 2003) (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). *But compare Morris v. Union Pac. R.R.,* 373 F.3d 896, 900-01 (8th Cir. 2004) (holding that adverse inference instruction sanction for destruction of engineer-dispatcher audiotape made at the time of accident was improper, distinguishing facts in *Stevenson*).

The analysis of the need for a "legal hold" is usually done by the legal department, but it may involve other departments as there may be a wide variety of reasons to institute hold orders (such as financial audits, compliance and litigation matters). A recommended practice is for the legal department to have a separate checklist of circumstances by which it considers whether a preservation obligation has been triggered and, if so, what steps need to be taken to identify the scope of the obligation and what has to been done to meet the obligation. The exact manner in which this is done may vary as long as there is a process by which circumstances can be evaluated to determine if there needs to be a suspension of ordinary destruction practices.

Comment 5.c.

An organization should identify persons with authority to suspend normal destruction procedures and impose a legal hold.

Organizations need to identify a chain of command to decide when normal records retention procedures should be suspended. Ideally, organizations can identify in advance one or more "point" persons responsible for managing this process. Contact information should be easily accessible to employees.

An organization's information and records management policy should provide specific direction concerning hold notices. This generally includes: (1) who has the authority to impose a legal hold on records otherwise scheduled for disposition; (2) who is responsible for communicating the legal hold requirements; (3) who is responsible for implementation; and (4) who has authority to determine that the need for a legal hold no longer exists. The policy could also provide a typical form of notice and channels for communicating when it is necessary to suspend the normal course of records retention and destruction. Of course, the content of the notice will vary depending on the particular circumstances. *See* Comment 5.e.

Comment 5.d.

An organization's information and records management procedures should recognize and may describe the process for suspending normal records and information destruction and identify the individuals responsible for implementing a legal hold.

Once a duty to preserve is triggered and a legal hold is required, the organization needs to take steps to implement the hold. Pre-established procedures set forth in the policy or other policy support materials can help clarify the requirements for a reasonably diligent search to identify, locate, collect and appropriately handle relevant documents when notice is received of actual or reasonably anticipated litigation, government investigation or audit. For all the reasons identified in describing why a multidisciplinary team may be

important to the successful launch of a retention program, *see* Comment 4.c. An effective litigation response team may often include persons in the organization responsible for oversight and administration of the information and records management policy, representatives from the legal department (preferably with some litigation experience), representatives of the IT department, other senior level managers or executives as may be appropriate to the matter or case, as well as sufficient staff to implement the response.

Litigation response issues the organization may wish to address include:

- How are potentially responsive records and other information identified?
- Who is involved in the identification?
- Who will be contacted?
- Where and how will records and other information subject to the legal hold be stored?
- Who collects and coordinates the retention of the records and other information subject to the legal hold?
- Whether and how to regularize and document the team process?
- What metadata, if any, may be material to a particular dispute and thus may need to be preserved?
- Whether records and other information must be "frozen" in a snapshot?
- Whether "point-in-time" information needs to be preserved on an ongoing basis (future snapshots), and, if so, when and how will this be done?
- Is there a particular need to preserve legacy on backup media or systems?

Comment 5.e.
Legal holds and procedures should be appropriately tailored to the circumstances.

Any suspension of the normal course of information and records retention and destruction—or "legal hold"—should be informed by legal judgment, should be tailored to the legal requirements of the case, and should apply only to the life of the litigation, investigation, audit or other circumstances giving rise to the suspension.

The obligation to preserve evidence does not require that all electronic information be frozen. *See Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) (organizations need not preserve "every shred of paper, every e-mail or electronic document, and every back-up tape"); *see also Wiginton v. Ellis,* No. 02 C 6832, 2003 WL 22439865, at *4 (N.D. Ill. Oct. 27, 2003) ("A party does not have to go to 'extraordinary measures' to preserve all potential evidence. … It does not have to preserve every single scrap of paper in its business.") (citing *China Ocean Shipping (Group) Co. v. Simone Metals Inc.*, No. 97 C 2694, 1999 WL 966443, at *3 (N.D. Ill. Sept. 30, 1999) and *Danis v. USN Communications, Inc.,* No. 98 C 7482, 2000 WL 1694325, at *32 (N.D. Ill. Oct. 20, 2000)). The scope of what is necessary to preserve will vary widely between and even within organizations depending on the nature of the claims and the information at issue. *See Zubulake,* 220 F.R.D. at 218 ("In recognition of the fact that there are many ways to manage electronic data, litigants are free

to choose how this task [of retaining relevant documents] is accomplished."); *see also The Sedona Principles: Best Practices, Recommendations and Principles for Addressing Electronic Document Production,* Principle No. 5 (Jan. 2004).

Accordingly, a legal hold should be limited in scope to only that information and records that may be relevant to the litigation. Decisions as to what should be held should be made as early in the process as practicable, and refined over time. Legal holds should not be all-inclusive, or encompass entire bodies of information and records just because it may be "easy" to seize the whole of a category or system. The legal hold must cover relevant electronic information and records, and the legal hold notice should specifically state that relevant electronic information and records must be preserved. *See The Sedona Principles: Best Practices, Recommendations and Principles for Addressing Electronic Document Production,* Principle No. 5 at 20 (Jan. 2004). In the civil litigation discovery context, the obligation to preserve and produce relevant evidence is generally understood to require that the producing party exert only reasonable efforts to identify and manage the relevant information readily available to it. *See Zubulake v. UBS Warburg LLC,* 220 F.R.D. 212, 217-18 (S.D.N.Y. 2003) (describing how contours of preservation obligation are defined); *Fennell v. First Step Designs, Ltd.,* 83 F.3d 526, 532 (1st Cir. 1996) ("In determining whether material is 'discoverable,' the court should consider not only whether the material actually exists, but the burdens and expenses entailed in obtaining the material."); MANUAL FOR COMPLEX LITIGATION, § 11.446 (4th ed.) ("For the most part, [computerized] data will reflect information generated and maintained in the ordinary course of business."). When the circumstances that gave rise to the hold cease to exist, the organization should determine whether the hold can be lifted in whole or in part, in order to alleviate further costs of preservation.

In particular circumstances, implementing a legal hold may also require a change to the organization's backup procedures for business continuation or disaster recovery. A legal hold should address what actions, if any, are to be taken to suspend recycling of disaster recovery backup tapes, either on a temporary or ongoing basis, pending further litigation developments. *Compare Zubulake*, 220 F.R.D. at 218 (holding that "as a general rule" litigation holds do not apply to "inaccessible" backup tapes, *i.e.*, those maintained solely for purposes of disaster recovery, but distinguishing backups used for information retrieval that would be subject to such holds) *with Applied Telematics, Inc. v. Sprint Communications Co*., No. 94-4603, 1996 WL 33405972, at *3 (E.D. Pa. Sept. 17, 1996) (holding defendant at fault "for not taking steps to prevent the routine deletion" of backup files); *and Keir v. UnumProvident Corp*., No. 02 Civ. 8781, 2003 WL 21997747, at *3 (S.D.N.Y. Aug. 22, 2003) (preservation obligations include backup tapes); *see also The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, Comment 5.h (Jan. 2004).[3]

In certain circumstances, legal hold procedures may require the suspension of certain automatic deletion programs or processes that continuously delete information without intervention (such as e-mail janitor programs). Suspension may be necessary when the organization knows that the program or process will lead to the loss of relevant records or other relevant information that is not otherwise preserved or available. Of course, if adequate policies and procedures are in place to preserve relevant information, there may be no need to alter the standard operating practices of the business (such as e-mail janitor programs).

3 When required to preserve backup tapes, an organization may elect to preserve a reasonable subset of previously created backup tapes (*i.e.*, keeping some combination of existing incremental, weekly or monthly backups), without in every case needing to indefinitely suspend the further recycling of backups. *See Zubulake*, 220 F.R.D. at 218 ("[i]f 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 is not otherwise available).

Illustration i. Under its records management policy and procedures, a company requires that its employees limit the quantity of electronic information that is stored, or limit the time that communications that do not constitute records of the organization can remain, in the employees' respective active e-mail accounts. Upon commencement of litigation, adequate steps are taken to inform the pertinent individuals to save relevant e-mail currently and in the future. The organization is not required to alter the policy, provided that the legal hold procedures are communicated and effective to preserve the relevant documents.

For examples of discussions of the various legal hold or preservation "scope" issues that have been identified in the case law, *see Proctor & Gamble Co. v. Haugen,* 179 F.R.D. 622, 631-32 (D. Utah 1998) (although no discovery order was yet in place, defendant was sanctioned for refusing to preserve corporate e-mails of five individuals it itself had identified as having information relevant to the pending litigation), *reversed in part by Proctor & Gamble Co. v. Haugen*, 222 F.3d 1262 (10th Cir. 2000); *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 relevant e-mails subsequent to the filing of the complaint even though pre-litigation e-mails were destroyed: "to hold that a corporation is under a duty to preserve all e-mail potentially relevant to any future litigation would be tantamount to holding that the corporation must preserve all e-mail"; such a holding, the court found, would be crippling to large corporations, which are often involved in litigation); *Willard v. Caterpillar, Inc.,* 40 Cal. App. 4th 892, 922-24, 48 Cal. Rptr. 2d 607 (Cal. Ct. App. 1995) (no duty to preserve documents relating to design of tractor that had been out of production for 20 years and where there were no known claims as to which the documents might be relevant; wrongfulness of evidence destruction is tied to temporal proximity between destruction and litigation interference, and foreseeability of harm to the non-spoliating litigant), *overruled on other grounds by Cedars-Sinai Med. Ctr. v. Superior Court*, 18 Cal. 4th 1, 74 Cal. Rptr. 2d 248, 954 P.2d 511 (Cal. Ct. 1998); *Moore v. Gen. Motors Corp.*, 558 S.W.2d 720, 735-37 (Mo. Ct. App. 1977) (declining to find spoliation where records were destroyed in accord with policy to destroy at end of model year and with no knowledge of pending litigation, there was no evidence manifesting fraud, deceit or bad faith, and plaintiff had made no effort to obtain through discovery once suit began); *see also Kucala Enters, Ltd. v. Auto Wax Co. Inc.,* No. 02 C 1403, 2003 WL 21230605, at *8 (N.D. Ill. May 27, 2003) (magistrate recommended that plaintiff's suit be dismissed and attorneys' fees awarded to defendant when court found that plaintiff had flagrantly violated duty to preserve by installing a software program designed to cleanse a hard drive of evidence; plaintiff's fear that defendant would not adhere to protective order was not justifiable and did not excuse duty to preserve); *McGuire v. Acufex Microsurgical, Inc.,* 175 F.R.D. 149, 153-56 (D. Mass. 1997) (no obligation to preserve all drafts of internal memos and no sanctionable conduct in deleting paragraph from personnel evaluation—even after state discrimination commission proceedings commenced; court found that employer had obligation to make sure that no false information was placed into personnel file; employer could review drafts of personnel memoranda and discard them when the editing related to obvious errors made by someone other than the accused harasser, and modified memorandum was promptly produced when it was later found on the home computer of the original author). *See also* Proposed Amendment to Fed. R. Civ. P. 37(f) (new) (steps taken to implement legal hold may be relevant in determining whether the routine deletion of information occurred in "good faith" and is thus entitled to "safe harbor" from sanctions), Report of the Advisory Committee on the Federal Rules of Civil Procedure to the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, at 128 (May 27, 2005), *available at* www.uscourts.gov.[4]

4 As of the publication of this document, Judicial Conference of the United States Advisory Committee on Civil Rules is considering the proposed amendments to the Federal Rules of Civil Procedure to address electronic discovery issues. It is unclear what new rules, if any, will ultimately be promulgated by the Supreme Court and Congress. If passed, the new rules would take effect no earlier than December 1, 2006.

Comment 5.f.

Effectively communicating notice of a legal hold should be an essential component of an organization's information and records management program.

Once events occur requiring that a legal hold be imposed, court decisions make clear that the notice should be communicated to appropriate custodians of affected records and individuals who may have other relevant information. Courts have identified the following factors as significant, so an organization imposing a legal hold should evaluate:

- ***The person providing the notice.*** Courts have repeatedly stated that document retention issues are significant matters for corporations and organizations and there must be sufficient attention and resources devoted to meeting preservation duties in light of the circumstances. *See Danis v. USN Communications, Inc.,* No. 98 C 7482, 2000 WL 1694325, at *39-41 (N.D. Ill. Oct. 20, 2000). In large organizations with thousands of employees, it should be sufficient that the notice come from senior representatives of the legal department or some other department charged with the responsibility for preserving records for the organization. *Cf. In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 F.R.D. 598, 612, 615-16 (D.N.J. 1997) (found that defendants' earlier preservation hold notices were inadequate and required senior management to advise employees of the pending litigation, provide them with a copy of the court order and inform them of their potential civil or criminal liability for noncompliance).

- ***The contents or scope of the notice.*** The notice need not be, and most likely should not be, a detailed catalog of documents to be retained, but instead can provide a sufficient description of the subject matter of the documents to be preserved that would allow the affected document custodians to segregate and preserve identified information and records. *See Wiginton v. Ellis,* No. 02 C 6832, 2003 WL 22439865, at *5 (N.D. Ill. Oct. 27, 2003) (initial notice sent to employees to preserve documents only pertaining to the one named plaintiff in a putative class action addressing employment issues was insufficient as it did not properly reflect scope of preservation obligation; broader revised notice was sufficient).[5]

- ***The means and extent of communicating the records hold.*** The notice does not need to reach all employees in the organization, only those necessary to preserve relevant information and records. The communication need not be disseminated beyond the scope of reasonable inquiry absent specific information and knowledge that requires otherwise. The notice should be communicated through means likely to reach the intended audience, and may include electronic and/or paper distribution. *See In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 F.R.D. 598, 612-13 (D.N.J. 1997) (noting that e-mails sent to employees did not contain bolded phrases like "DO NOT DESTROY DOCUMENTS," that the e-mails did not mention the specific pending litigation or the possibility that failure to comply could give rise to civil or criminal penalties, that not all employees had e-mail access to receive the e-mails sent, and that not all notices were circulated in paper format as well as electronic).

Illustration ii. Under its policy, a potential producing party enlists the assistance of its employees or agents who are identified as possibly having relevant information by informing them of the nature of the controversy and the time frame involved, and by providing them with

5 This aspect of the *Wiginton* case is troubling for it uses a subsequent remedial measure (a more precise preservation notice) as evidence that the first notice was insufficient. *Wiginton v. Ellis*, No. 02 C 6832, 2003 WL 22439865, at *5 (N.D. Ill. Oct. 27, 2003).

a method of accumulating and updating (where disputes are ongoing) copies of the relevant information. The appropriate individuals are instructed to preserve relevant information for the duration of the controversy and steps are established to follow up with the identified individuals and secure the information. The organization has likely fulfilled its obligations.

- ***Whether notice should be sent to third parties.*** Consideration should be given to sending the notice of the legal hold to third parties if such third parties possess documents or data that effectively are in the possession, custody or control of the producing party.

- ***Updated notices.*** Consideration should be given as to whether notices of the legal hold should be updated as the litigation proceeds (*e.g.*, where new parties or claims are added or eliminated). Care must be given, however, to ensure appropriate consistent direction among all preservation notices. In certain circumstances, organizations may want to consider repeating notices or periodic general reminders that employees need to adhere to previously issued legal holds. *Cf. Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243, 2004 WL 1620866, at *9 (S.D.N.Y. July 20, 2004) (recommending periodic re-issuing of litigation hold notices).

Comment 5.g.
Documenting the steps taken to implement a legal hold may be beneficial.

Organizations should consider ways in which the legal hold process—either generally or in a given case—is recorded. This should usually include a copy of any legal hold notice(s) that have been issued, and a distribution list for the notice(s). Some organizations may wish to create checklists which outline the steps taken from the point of notice through the decision to release a legal hold. Such documents may assist in the development of affidavits or testimony which might be required should the preservation process be challenged. Some organizations require employees to certify receipt of, and compliance with, legal hold instructions. Other organizations rely on the legal hold notice combined with other steps, such as witness interviews, to ensure appropriate preservation steps have been taken. Regardless of the steps taken, a record of compliance can be very useful in defending any challenges to the organization's good faith efforts to meets its preservation obligations. *Cf. Zubulake v. UBS Warburg LLC,* No. 02 Civ. 1243, 2004 WL 1620866, at *9-10 (S.D.N.Y. July 20, 2004) (noting roles of counsel and client in implementing legal hold notices and procedures).

Although documenting preservation efforts is a recommended practice, there is no legal requirement mandating the creation of such a "paper trail." Likewise, the absence of such documentation in a particular instance or organization should not be viewed as evidence that the organization did not act in good faith or that its efforts were not sufficient to meet its legal obligations.

Comment 5.h.
If an organization takes reasonable steps to implement a legal hold, it should not be held responsible for the acts of an individual acting outside the scope of authority and/or in a manner inconsistent with the legal hold notice.

As noted elsewhere, courts have imposed severe sanctions on organizations that have been found to have allowed the spoliation of evidence by either reckless or intentional conduct attributed to the organization. *See United States v. Philip Morris USA Inc.,* 327 F. Supp. 2d 21, 25-26 (D.D.C. 2004) (where 11 senior executives failed to follow internal procedures for preservation, court barred witness from testifying at trial and imposed

total sanctions of $2.75 million); *GE Harris Railway Electronics, LLC v. Westinghouse Air Brake Co.*, 2004 U.S. Dist. LEXIS 16329, 2004 WL 1854198 (D. Del. Aug. 18, 2004) (adverse inference and contempt finding warrant $1.8 million fine); *Kucala Enters., Ltd. v. Auto Wax Co. Inc.,* No. 02 C 1403, 2003 WL 21230605, at *8 (N.D. Ill. May 27, 2003). Some courts have stated that negligent conduct may be sufficient to warrant sanctions in certain circumstances. *See Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99 (2nd Cir. 2002). These courts have not, however, explicitly described how a party's good faith and reasonable efforts to implement legal hold procedures may insulate it from liability for the spoliation of evidence by employees who have failed to follow the organization's policies and directives. *Compare Convolve, Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162, 177 (S.D.N.Y. 2004) (declining to impose sanctions where failure to preserve was not intentional, and declining to require preservation of "ephemeral" information where to do so would require heroic efforts far beyond the regular course of business) *with In re Adelphia Communications Corp.*, 327 B.R. 175, 180 (Bankr. S.D.N.Y. 2005) ("Thus the court is constrained to disagree with the Creditors' Committee's broad statement, citing to page 2134 of the [Supreme Court Reporter's publication of the *Arthur Andersen* decision], that *Arthur Andersen* 'makes clear that a company may not be convicted where the wrongdoing is not international and pervasive, and that the acts of a few cannot be imputed to a corporation that otherwise lacks criminal intent.' *Arthur Andersen* makes clear that wrongdoing must be intentional, but that is as far as it goes.").

The recognition of the availability of a "safe harbor" against culpability in such circumstances is essential, and the proposed amendments to the Federal Rules of Civil Procedure (still working their way through the approval process as of publication) would provide a limited safe harbor for the loss of information through the routine, good faith operation of computer systems. The Advisory Committee notes make clear that an organization's efforts to impose a legal hold should be considered in determining "good faith." *See* Report of the Advisory Committee on the Federal Rules of Civil Procedure to the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, at 125-29 (May 27, 2005; rev. ed. July 25, 2005), *available at* www.uscourts.gov. As is abundantly clear from the body of this document, the nature and volume of electronic documents is such that there is no possibility that any preservation system can be perfect. *See* Comments 1.b and 1.c, *see also Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) ("Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every e-mail or electronic document, and every backup tape? The answer is clearly, 'no.' Such a rule would cripple large corporations, like UBS, that are almost always involved in litigation."); *Wiginton v. Ellis*, No. 02 C 6832, 2003 WL 22439865, at *4, *7 (N.D. Ill. Oct. 27, 2003) (organization "does not have to preserve every single scrap of paper in its business"; "CBRE did not have the duty to preserve every single piece of electronic data in the entire company."). In addition, economic incentives for the creation of reasonable and effective litigation hold procedures will be eroded if there is no benefit absent a guarantee that the process will be perfect.

Consistent with the legal authority examined in this document, although no court has expressly so ruled, the authors believe that if an organization takes reasonable and appropriate steps to ensure that relevant information is preserved, but an employee engages in conduct inconsistent with the organization's directions (express and implied), it *may* be appropriate to hold the individual, but not the organization, responsible provided that the organization can demonstrate it applied and enforced its policy and did not condone or adopt the actions of the employee. *See In re Adelphia Communications Corp.*, 327 B.R. at 180 (in rejecting Creditors' Committee for a broad interpretation of the *Arthur Andersen* decision to insulate corporations from criminal liability for acts of a limited number of employees when the corporation lacks criminal intent, court nevertheless noted that the proposition advanced by the Creditors' Committee "… may be what the law already is, and may be what the law should be …"). At a minimum, if the organization took reasonable steps in good faith to preserve evidence, the organization will, typically, not be held accountable for "willful"

spoliation, which carries with it the most severe penalties. Courts should examine the specific facts and circumstances of each case before determining that an organization should be held responsible for spoliation despite the implementation in good faith of a demonstrable and reasonable "legal hold" process.

Comment 5.i.
Legal holds are exceptions to ordinary retention practices and when the exigency underlying the hold no longer exists (*i.e.*, there is no continuing duty to preserve the information), organizations are free to lift the legal hold.

An organization's policy and procedures can explain not only who in the organization has authority for determining that the need for a legal hold no longer exists, but also what factors or information should be considered, and what procedures should be followed, to remove the legal hold. Considerations may include:

- The form and content of notice that the legal hold has been lifted;
- Whether there is a post-case obligation to maintain some records or other information pursuant to normal retention schedules or otherwise;
- Whether the records or other information that can now be destroyed, are subject to another legal hold, or may be needed for another special purpose (*e.g.*, needed in whole or in part for other litigation);
- Whether the underlying litigation that has been resolved gives rise to the reasonable anticipation of other similar litigation;
- Whether records or information in third-party custody can be destroyed; and
- Whether the records or other information can be disposed of as soon as the legal hold is lifted, or whether the organization should wait until the next scheduled disposition.

Appendix A: Table of Authorities

This Table lists those authorities cited in the text of the Guidelines and Commentary (excluding appendices).

Federal Cases

Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), Pub. L. No. 108-159 117 Stat. 1952.....

Health Insurance Portability and Accountability Act (HIPAA) of 1996 .....

Rules

16 C.F.R. § 682, *et seq.*.....

17 C.F.R. pts. 228, 229, 232, 240, 249, 270 & 274 .....

Fed. R. Civ. P. 1 .....

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

FED. R. EVID. 1002 .....

FED. R. EVID. 1003 .....

Other Authorities

In the Matter of Banc of Am. Sec. LLC, SEC Admin. Proc. File No. 3 11425, Exchange Act Release No. 34-49386, 82 SEC Docket 1264 (Mar. 10, 2004).....

SEC v. Lucent Technologies Inc., SEC Accounting & Auditing Enforcement Release No. 2016, 82 SEC Docket 3224 (May 17, 2004) .....

U.S. Dist. Ct. Ark. L.R. 26.....

U.S. Dist. Ct. N.J. L.R. 26.....

U.S. Dist. Wyo. L.R. 26 .....

Miscellaneous

AMA/ePolicy Institute Research *2004 Workplace E-Mail and Instant Messaging Survey Summary*, *available at* http://www.epolicyinstitute.com/survey/survey04.pdf .....

AmSouth Bank Agrees to Forfeit $40 Million, U.S. Department of Justice, United States Attorney, S.D. Miss.; (Oct. 12, 2004), *available at* http://www.usdoj.gov/usao/mss/documents/pressreleases/october2004/amprsrels.htm .....

ANSI Standard IT9.23-1998 .....

ARMA Glossary of Records and Information Management Terms (ANSI/ARMA 10-1999: Sept. 26, 2000)....

Charles A. Lovell & Roger W. Holmes, *The Dangers of Email: The Need For Electronic Data Retention Policies,* 44 R.I.B.J. 7 (Dec. 1995) .....

Charles M. Dollar, *Authentic Electronic Records: Strategies for Long-Term Access* (Cohasset Associates 2002) .....

Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364) 1, 10 (Dec. 18, 2000), *available at* http://www.europarl.eu.int/charter/pdf/text_en.pdf .....

Christopher V. Cotton, *Document Retention Programs for Electronic Records: Applying a Reasonableness Standard to the Electronic Era,* 24 Iowa J. CORP. L. 417 (1999).....

Commission Decision 2000/520/EC of 26.7.2000 - O. J. L 215/7 of 25.8.2000" pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal date provided by the Safe Harbour Privacy Principles.....

Council Direct 95/46 *on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data,* 1995 O.J. (L 281) 31 (Nov. 23, 1995).....

Daniel L. Pelc and Jonathan M. Redgrave, *Challenges for Corporate Counsel in the Land of E Discovery: Lessons from a Case Study*, 3 ANDREWS E-BUSINESS LAW BULLETIN 1 (Feb. 2002) .....

David O. Stephens and Roderick C. Wallace, *Electronic Records Retention: Fourteen Basic Principles*, INFO MGMT. J., October 2000 .....

Default Standard for the Discovery of Electronic Documents, ("E-Discovery") (D. Del. 2004) (J. Robinson), *available at* www.ded.uscourts.gov/SLRmain.htm .....

Donald S. Skupsky, *Applying Records Retention to Electronic Records,* INFO MGMT. J., July 1999 .....

Donald S. Skupsky, *Legal Issues in Records Retention and Disposition Programs, available at* http://www.irch.com/articles/articl05.pdf.....

Donald Skupsky, *Establishing Records Retention Periods for Electronic Records*, INFORMATION RECORDS CLEARINGHOUSE (2000), available at http://www.irch.com/articles/articl09.pdf .....

Electronic Records Archives Concept of Operations (CONOPS v. 4.0); National Archives and Records Administration Electronic Records Archives Program Management Office, July 27, 2004, *available at* http://www.archives.gov/era/pdf/concept-of-operations.pdf .....

Eric Auchard, "Search concepts, not keywords, IBM tells business" (Reuters Aug. 8, 2005), *available at* http://www.computerworld.com/databasetopics/businessintelligence/datawarehouse/story/0, 10801,103763,00.html?SKC=datawarehouse-103763. .....

Ian C. Ballon, *Spoliation of E-Mail Evidence: Proposed Intranet Policies and a Framework for Analysis*, CYBERSPACE LAWYER (March 1999) .....

ISO 15489-1 .....

ISO 15489-2 .....

ISO 18492 .....

John C. Montaña, *Legal Obstacles to E-Mail Message Destruction* (ARMA Int'l Educ. Found. 2003).....

Jonathan M. Redgrave, R. Christopher Cook & Charles R. Ragan, *Looking Beyond Arthur Andersen: The Impact on Corporate Records and Information Management Policies and Practices,* The Federal Lawyer (Sept. 2005).....

MANUAL FOR COMPLEX LITIGATION, § 11.446 (4th ed.).....

Marianne Swanson *et al.*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, CONTINGENCY PLANNING GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS (Dep't of Commerce 2002).....

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

Opinion 8/2004 on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America (30.9.2004) .....

Out-Law News, *Rambus Lawsuit Against Infineon Dismissed*, Feb. 3, 2005 .....

Peter Lyman & Hal R. Varian, *How Much Information 2003, available at* http://www.sims.berkeley.edu/research/projects/how-much-info-2003.....

Press Release, "Commission decisions on the adequacy of the protection of personal data in third countries" *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm .....

Proposed Amendments to Fed. R. Civ. P. 26 promulgated by the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States (August 2004).....

Randolph A. Kahn & Barclay T. Blair, *Information Nation: Seven Keys to Information Management Compliance* (AIIM 2004) .....

Randolph A. Kahn and Barclay T. Blair, *Information Nation Warrior: Information and Managerial Compliance Boot Camp* (AIIM 2005) .....

Report of the Advisory Committee on the Federal Rules of Civil Procedure to the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States (May 27, 2005).....

Report of the Advisory Committee on the Federal Rules of Civil Procedure to the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States (May 27, 2005; rev. ed. July 25, 2005) .....

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

Retention Management for Records and Information (ANSI/ARMA 8-2005: Feb. 7, 2005).....

Sasha Talcott, *Bank Data Loss May Affect 60 Officials*, Boston Globe, Feb. 27, 2005 .....

Sheila Taylor, *Benchmarking for Records Management Excellence*, MUNICIPAL WORLD (Jan. 2003), *available at* http://www.condar.ca/CONDAR%20Articles/article%2015%20RM%20Benchmarking.pdf .....

Teens and Technology: Youth are Leading the Transition to a Fully Wired and Mobile Nation," PEW/Internet, July 27, 2005, *available at* http://www.pewinternet.org/PPF/r/162/report_display.asp) ....

The Sedona Principles: Best Practices, Recommendations and Principles for Addressing Electronic Document Production (Jan. 2004) .....

Thomas Y. Allman, *Fostering a Compliance Culture: The Role of The Sedona Guidelines*, THE INFORMATION MANAGEMENT JOURNAL (ARMA April/May 2005) .....

Timothy Q. Delaney, *Email Discovery: The Duties, Danger and Expense*, 46 FED. LAW. 42 (Jan. 1999) .....

Vital Records: Identifying, Managing and Recovering Business Critical Records (ANSI/ARMA 5-2003: Mar. 13, 2003) .....

Appendix B: Standards

The following entries constitute a selected list of organizational Web sites providing information on international, national, and state government standards relevant to electronic records, with citations to specific standards where applicable. The list does not purport to be comprehensive; in many cases, the Web sites themselves operate as portals to much richer array of information located on the Web. The entries below contain a current direct link pointing to the "standards" information on the Web site; however, given the frequency of Web page updates and the possibility of broken links to sub-URLs, a home page also has been provided for each main organization. Short descriptions for the listed organizations have been mostly taken verbatim from the Web sites themselves. [All websites were last accessed on 8/16/05.]

1. AIIM (Enterprise Content Management Association)

- http://www.aiim.org
- http://www.aiim.org/standards.asp?ID=24488

  AIIM Standards is comprised of twenty-plus committees and working groups. Over 80 of AIIM's standards, recommended practices and technical reports have been drafted and approved by ANSI. AIIM holds the secretariat for ISO/TC 171 SC2, Document Imaging Applications, and Application Issues. AIIM is also the administrator for the U.S. Technical Advisory Group (TAG) to ISO TC 171, Document Imaging Applications that represents the United States at international meetings.

2. American National Standards Institute (ANSI)

- http://www.ansi.org
- http://www.ansi.org/standards_activities/overview/overview.aspx?menuid=3

  ANSI is a private, non-profit organization (501(c)(3)) that administers and coordinates the U.S. voluntary standardization and conformity assessment system.

- ANSI/AIIM TR31, Performance Guideline for the Legal Acceptance of Records Produced by Information Technology

3. ARMA (The Association for Information Management Professionals)

- http://www.arma.org
- http://www.arma.org/standards/index.cfm

  Standards development is a major activity for ARMA International at both the national and international levels. ARMA is an accredited standards development organization with the American National Standards Institute (ANSI). ARMA also participates in applicable ISO standards development committees such as TC 46/SC 11 Archives/Records Management.

4. Cohasset Associates, Inc.

- http://www.cohasset.com
- http://www.merresource.com/library/index.php?dir=policies_and_guidelines

  Cohasset is a private consulting firm specializing in document-based information management, and is host to the Managing Electronic Records (MER) Conferences.

5. Committee on Institutional Cooperation (CIC), University Archivists Group (UAG)

- http://www-personal.umich.edu/%7Ederomedi/CIC/cic.htm

  This website sets out CIC UAG Standards for an Electronic Records Policy.

6. The Document Site

- http://www.thedocumentsite.co.uk
- http://www.thedocumentsite.co.uk/RM_resources.html

  The site is published and maintained by Reynold Leming, Managing Director of Mint Business Solutions Ltd., an information management consultancy.

7. Electronic Media Group

- http://aic.stanford.edu/sg/emg/

  The mission of the Electronic Media Group (EMG) is two fold: (1) preservation of electronic art, electronic-based cultural materials and tools of creation; and (2) to provide a means for conservators and related professionals to develop and maintain knowledge of relevant new media and emerging technologies.

8. Electronic Resource Preservation and Access Network (ERPANET)

- http://www.erpanet.org

  The European Commission—funded ERPANET Project will establish an expandable European Consortium, which will make viable and visible information, best practice and skills development in the area of digital preservation of cultural heritage and scientific objects. ERPANET will provide a virtual clearinghouse and knowledge base on state-of-the-art developments in digital preservation and the transfer of that expertise among individuals and institutions.

9. IEEE Computer Society

- http://www.computer.org
- http://www.computer.org/standards

With nearly 100,000 members, the IEEE Computer Society is the world's leading organization of computer professionals. Founded in 1946, it is the largest of the 37 societies of the Institute of Electrical and Electronics Engineers (IEEE).

The Society is dedicated to advancing the theory, practice, and application of computer and information processing technology.

10. Indiana University Bloomington Libraries, University Archives

- http://www.libraries.iub.edu/index.php?pageId=3313

Website includes citations to white papers and standards on methodologies for designing record-keeping systems, evaluating information systems as record-keeping systems, functional requirements for record-keeping systems, record-keeping metadata specifications, and records policies and guidelines.

11. International Council on Archives

- http://www.ica.org

The International Council on Archives (ICA) is a decentralized organization governed by a General Assembly and administered by an Executive Committee. Its branches provide archivists with a regional forum in all parts of the world (except North America); its sections bring together archivists and archival institutions interested in particular areas of professional interest; its committees and working groups engage experts to solve specific problems. The ICA Secretariat serves the administrative needs of the organization and maintains relations between members and cooperation with related bodies and other international organizations.

- http://www.ica.org/biblio.php?pbodycode=CER&ppubtype=pub&plangue=eng

ICA Committee on Current Records in Electronic Environments

- http://www.ica.org/biblio.php?pbodycode=CDS&ppubtype =pub&plangue=eng

ICA Committee on Descriptive Standards

12. International Organization for Standardization

- http://www.iso.org

A network of national standards institutes from 148 countries working in partnership with international organizations, governments, industry, business and consumer representatives. The source of ISO 9000, ISO 14000 and more than 14,000 International Standards for business, government and society.

- ISO 15489-1 and 2:2001(E), International Standard: Information and Documentation - Records Management

13. International Research on Permanent Authentic Records in Electronic Systems (InterPARES Project)

- http://www.interpares.org
- http://www.interpares.org/links.htm

The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) aims to develop the theoretical and methodological knowledge essential to the long-term preservation of authentic records created and/or maintained in digital form. This knowledge should provide the basis from which to formulate model policies, strategies and standards capable of ensuring the longevity of such material and the ability of its users to trust its authenticity.

14. MoReq ("Model Requirements") Project

- http://www.inform-consult.com/services_moreq.asp
- http://www.cornwell.co.uk/moreq

Websites describing an EEC model records management requirement and specification.

15. Monash University, Australia, School of Information Management and Systems

- http://www.sims.monash.edu.au/index.html
- http://www.sims.monash.edu.au/research/rcrg/links.html

The mission of the School of Information Management and Systems is to advance through teaching, research and community engagement, the organization, application, management and use of information and information technology, and to enhance our understanding of the impact of information on individuals, organizations, institutions, and society.

16. NAGARA (National Association of Government Archives and Records Administrators)

- http://www.nagara.org
- http://www.nagara.org/links.html

NAGARA is a professional organization dedicated to the effective use and management of government information and publicly recognizing their efforts and accomplishments.

17. National Archives (United Kingdom)

- http://www.nationalarchives.gov.uk
- http://www.nationalarchives.gov.uk/electronicrecords/advice/default.htm

Standards on the development and best practices for e-records management systems, includes toolkits and suggestions for developing corporate policies and inventory systems.

- http://www.nationalarchives.gov.uk/electronicrecords

18. National Archives of Australia

- http://www.naa.gov.au
- http://www.naa.gov.au/recordkeeping/rkpubs/summary.html (links to record-keeping publications)

19. New South Wales State Records

- http://www.records.nsw.gov.au/publicsector/erk/electronic.htm (electronic record-keeping)

20. OASIS

- http://www.oasis-open.org/home/index.php

  Non-profit consortium coordinating development of e-business standards; parent organization for LegalXML.

21. Open Archives Initiative

- http://www.openarchives.org/index.html
- http://www.oaforum.org/oaf_db/list_db/list_protocols.php

  The Open Archives Initiative develops and promotes interoperability standards that aim to facilitate the efficient dissemination of content. The Open Archives Initiative has its roots in an effort to enhance access to e print archives as a means of increasing the availability of scholarly communication.

22. Research Libraries Group

- http://www.rlg.org
- http://www.rlg.org/en/page.php?Page_ID=553

  Current Projects, including Encoded Archival Context Activities and Encoded Archival Description activities.

  The Research Libraries Group (RLG) is an international consortium of universities and colleges, national libraries, archives, historical societies, museums, independent research collections and public libraries. Its mission is to "improve access to information that supports research and learning" through collaborative activities and services that include organizing and preserving as well as sharing information resources.

23. Society of American Archivists

- http://www.archivists.org
- http://www.archivists.org/governance/handbook/standards_com.asp (Standards Committee)

  The Standards Committee is responsible for overseeing the process of developing, implementing, and reviewing standards pertinent to archival practice and to the archival profession and for providing for effective interaction with other standards-developing organizations whose work affects archival practice.

- http://www.archivists.org/catalog/stds99/index.html
  (Standards for Archival Description Handbook)
- http://www.archivists.org/assoc-orgs/index.asp (links to related associations)
- http://www.loc.gov/ead/ (Encoded Archival Description website)
- http://www.archivists.org/saagroups/ers/index.asp (Electronic Records section)

24. State University of New York, Albany, Center for Technology in Government

- http://demo.ctg.albany.edu/projects/mfa

  The Center for Technology in Government works with governments to develop information strategies that foster innovation and enhance the quality and coordination of public services, carrying out this mission through applied research and partnership projects that address the policy, management and technology dimensions of information use in the public sector. Website contains references to publications concerning functional requirements for electronic record-keeping.

25. University of Michigan/University of Leeds, CAMiLEON Project

- http://www.si.umich.edu/CAMILEON/index.html

  The CAMiLEON Project is developing and evaluating a range of technical strategies for the long-term preservation of digital materials. User evaluation studies and a preservation cost analysis are providing answers as to when and where these strategies will be used. The project is a joint undertaking between the Universities of Michigan (USA) and Leeds (UK) and is funded by JISC and NSF.

26. University of Pittsburgh, School of Information Sciences

- http://www.archimuse.com/papers/nhprc/meta96.html

  Metadata Specifications Derived from Functional Requirements: A Reference Model for Business Acceptable Communications.

27. University of Virginia Library and Cornell University Fedora Project

- http://www.fedora.info

The Fedora project was funded by the Andrew W. Mellon Foundation to build an open-source digital object repository management system based on the Flexible Extensible Digital Object and Repository Architecture (Fedora). The new system demonstrates how distributed digital library architecture can be deployed using web-based technologies, including XML and Web services. Fedora was jointly developed by the University of Virginia and Cornell University.

28. U.S. Department of Agriculture, Records Management

- http://www.ocio.usda.gov/records/index.html

Comprehensive web site with links to federal resources.

29. U.S. Department of Defense, 5015.2 Standard

- http://www.dtic.mil/whs/directives/corres/html/50152std.htm

Design Criteria Standard for Electronic Records Management Software Applications (June 2002). This Standard is issued under the authority of DoD Directive 5015.2, "Department of Defense Records Management Program," March 6, 2000, which provides implementing and procedural guidance on the management of records in the Department of Defense. This Standard sets forth mandatory baseline functional requirements for Records Management Application (RMA) software used by DoD Components in the implementation of their records management programs; defines required system interfaces and search criteria to be supported by the RMAs; and describes the minimum records management requirements that must be met, based on current National Archives and Records Administration (NARA) regulations.

- http://jitc.fhu.disa.mil/recmgt/standards.htm

"Functional baseline requirements" study that provides additional requirements and data element descriptions for records management metadata.

30. U.S. Environmental Protection Agency (Records Management Website)

- http://www.epa.gov/records/policy/index.htm (contains links to additional sites)

31. U.S. Library of Congress, Metadata Encoding & Transmission Standard (METS)

- http://www.loc.gov/standards/mets

The METS schema is a standard for encoding descriptive, administrative, and structural metadata regarding objects within a digital library, expressed using the XML schema language of the World Wide Web Consortium. The standard is maintained in the Network Development and MARC Standards Office of the Library of Congress, and is being developed as an initiative of the Digital Library Federation.

32. U.S. National Aeronautics and Space Administration, Science Office of Standards and Technology

- http://ssdoo.gsfc.nasa.gov/nost
- http://ssdoo.gsfc.nasa.gov/nost/isoas

Summarizing U.S. efforts towards ISO archiving standards.

33. U.S. National Archives and Records Administration

- http://www.archives.gov
- http://www.archives.gov/records-mgmt/index.html

http://www.archives.gov/records-mgmt/initiatives/

Providing links to various electronic records initiative projects.

34. U.S. National Institute of Standards and Technology (NIST)

- http://www.nist.gov
- http://www.itl.nist.gov/iaui

The Information Access Division (IAD), part of NIST's Information Technology Laboratory, provides measurements and standards to advance technologies dealing with access to multimedia and other complex information.

- http://www.itl.nist.gov

The Information Technology Laboratory (ITL) works with industry, research, and government organizations to make this technology more usable, more secure, more scalable, and more interoperable than it is today. ITL develops the tests and test methods that both the developers and the users of the technology need to objectively measure, compare and improve their systems.

35. Utah Division of State Archives

- http://archives.utah.gov/recmanag/electronic.htm

Comprehensive web site listing electronic record-keeping related resources including policies and programs from all 50 states.

36. World Wide Web Consortium (W3C)

- http://www.w3c.org
- http://www.w3c.org/RDF (Resource Description Framework)

- http://www.w3c.org/Consortium/Activities

  The World Wide Web Consortium (W3C) develops interoperable technologies (specifications, guidelines, software, and tools) to lead the Web to its full potential. W3C is a forum for information, commerce, communication, and collective understanding.

37. XML.ORG

- http://www.xml.org

  XML standards for specific industry areas.

Appendix C: Summary of Cohasset Associates' 2005 Survey Results

Co-sponsored by ARMA International and AIIM International

Dramatic events have played out in boardrooms, courts and the media in the last several years focusing the attention of lawmakers, lawyers, regulators, auditors and investors on one critical aspect of business—the management of information and records. This awakening regarding the intrinsic value of information assets has resulted in a special need to refocus on the processes by which business records are managed, particularly those that are produced and stored electronically.

The impetus for *The Sedona Guidelines* originated primarily within the legal community, but studies and surveys related to information and records management topics spearheaded by those in the records management and information technology industries were an important part of corporate consciousness-raising. The survey summarized in this Appendix, while not a catalyst for the development of the Guidelines, highlights why organizations should consider the Guidelines' recommendations to improve the management of electronic information and records.

Three leading United States organizations in the field of records and information management teamed together in spring of 2005 to assess the current state of electronic records management. Cohasset Associates, Inc., a management consulting firm specializing in records management, conducted the research, performed the analysis and prepared an industry White Paper containing the complete findings and analysis. ARMA International and AIIM, the two primary professional organizations dedicated to records management, co sponsored the survey. The respondents were more than 2,000 members of ARMA and AIIM, recent attendees at the annual National Conference on Managing Electronic Records (MER), as well as subscribers to the Records Management LISTSERV--those with the best understanding of the survey's subject matter.

The 2005 survey results come from 34 close-ended, issue-based questions. To optimize measurement of trends over time, most of the questions were identical or very similar to the questions in three similar surveys conducted and reported in 1999, 2001 and 2003 by Cohasset Associates.

Significant challenges and numerous shortfalls in the records management processes are shown in the surveys findings and the trends over time:

- Nearly one-third (32%) of respondents evaluate their records management program as either "marginal" (11%) or "fair" (21%) - the two lowest categories in a five point semantic scale. [The cumulative assessment is a 22% improvement from 2003.]

- Nearly all survey respondents (99%) believe the current process for managing electronic records in their organizations will impact future litigation. This data is a 9% improvement over the 2003 data which reported that 93% believed it would be important in future litigation.

- Nearly half (49%) of the respondent's organizations do not have any formal e-mail retention policy and this is a 17% improvement.
- A significant percentage (43%) of the organizations represented do not include electronic records in their retention schedules. This is a 9% improvement from the 2003 survey.
- Some 29% of the respondents reported that their organizations follow their retention schedules either "not regularly" (18%) or only "when time permits" (11%).
- Only 57% of the organizations have a formal plan to respond to discovery requests for records, which is a 24% improvement.
- 53% reported that electronic records are not included in their organization's records holds, and this is an 18% improvement.
- Some 49% or respondents were either "not confident at all" (21%) or only "slightly confident" (28%) that their organization could demonstrate its electronic records were accurate, reliable and trustworthy many years after they were created.
- Many organizations (67%) experienced "some" (38%), "considerable" (21%) or "great" (9%) difficulty in finding and retrieving information from back-up and archival storage media in response to court-ordered discovery.
- In over one-third (39%) of the organizations the IS/IT department defines the retention schedules for archival and back-up media and at 61% of the organizations represented, IS/IT is responsible for the day-to-day management of electronic records; however well over half (57%) of the respondents do not believe that their organization's IS/IT staff realizes that it will have to migrate many of the organization's electronic records in order to comply with established retention policies; 69% do not have a records migration plan in place; and 70% do not believe their IS/IT colleagues really understand the concept of "life cycle" regarding the management of the organization's electronic records.
- New data not sought in the prior surveys indicated that 27-72% of respondents (records management professionals, those primarily responsible for overseeing the organization's application of retention schedules) do not know the degree to which schedules were being applied to archival and back-up electronic records storage media. Additionally only 32% of records management professionals have responsibility for archiving and back-up media in their organizations.

The complete survey results are reported in The "2005 Cohasset ARMA AIIM Electronic Records Management Survey" prepared by Cohasset Associates, Inc. (October 2005), which is available at http://www.merresource.com/whitepapers/survey.htm. Additional information regarding Cohasset & Associates is available at www.cohasset.com.

Appendix D: Survey of Data Within an Organization

An organization's information and records management policy should be based on an accurate and complete understanding of the sources and types of electronic records generated, received and used within the organization, as well as an overall assessment of the practices in place regarding the use, retention, storage, preservation and destruction of records generally. During this assessment, the organization should review its current records program: how records are created and maintained; how records disposition decisions are made and implemented; and how records critical to the organization are protected.

Specifically, the organization should plan to gather information on its:

- Size, structure, locations, industry;
- Regulatory requirements for record-keeping;
- Current records management policies and procedures;
- Information systems infrastructure; and
- Methods for ensuring compliance with policies and procedures.

Many models for such record-keeping surveys exist, but no one template can be taken as a talisman for every organization. This Appendix provides a sample that can be used as a starting point by organizations addressing records management issues, with particular emphasis on electronic information. Note, however, that this survey is not exhaustive and an organization should consult with individuals equipped to assist in a comprehensive review of records management programs and policies. Other samples that may also be useful as a guide in creating a customized assessment tool include:

- National Archives and Records Administration (NARA)'s Records Management Self-Evaluation Guide, *available at* http://www.archives.gov/records_management/publications/records_management_self_evaluation_guide.html#intro
- National Archives of Australia's Record-keeping Policy Checklist, *available at* http://www.naa.gov.au/recordkeeping/overview/policy/check.html
- The Center for Technology in Government's The Records Requirements Analysis and Implementation Tool, *available at* http://www.ctg.albany.edu/publications/guides/rrait

For organizations that wish to assess their records management, particularly in comparison to the requirements in ISO 15489-1, ARMA International has developed an online assessment tool. It is a high level (rather than in-depth) assessment, but will be valuable in the initial stages of program assessment or development. More information on this assessment product (RIM e-Assessment) can be found on the ARMA website (www.arma.org/standards).

I. Written Policies

A. Obtain and review any existing records management policies and directives for all media (paper and electronic).

1. Evaluate policy(ies)

a. Is it written?

b. Is it contained in a single document?

c. Is it clear?

d. Is it well distributed and easily accessible?

2. What is the scope of the policy?

a. Does it apply to all kinds of information? (*i.e.*, paper, e-mail, word processing documents, spreadsheets, databases)

b. Does it apply globally?

c. Does it apply to subsidiaries and affiliates?

d. Does it apply to records in the possession of contractors, outside counsel, etc.?

II. Identify business needs and regulatory and legal responsibilities

A. What is the company's:

1. size? (number of employees)

2. structure? (public or private; parent/subsidiary/sister co.)

3. locations? (national and international)

4. industry?

5. products / services?

6. perceived core business functions?

B. Determine operational and regulatory factors

1. What are the business or legal considerations that drive record-keeping?

2. How does the nature of the business affect the creation and management of information that is vital to business functions?

3. How does the industry in which the business operates affect the kind of information that the business must retain for legal reasons?

4. Does the company belong to any industry or trade organizations, or have another designation, which imposes certain guidelines, standards or requirements?

5. Does the company's specific structure, needs, legal duties or other considerations require that document management policies for electronic records be distinguished from those used for paper records?

C. Obtain and review any existing records retention schedules

1. Who has authority to create or modify schedules?

2. What is the process for creating or modifying schedules?

3. How are the schedules organized (by business, by function, by topic, etc.)?

4. Do the retention schedules distinguish certain types of documents as "records" and other types of documents as something other than "records"?

5. Do the retention schedules apply regardless of storage medium? (paper, electronic, microfilm, CD, file server, etc.)

6. Are there "conditional" retention schedules (*i.e.*, triggered by a future event)? (*e.g.*, "Life of system" or "3 years after termination of employment")

7. If an employee is uncertain what retention category applies to a record, what is the mechanism to provide an answer?

8. Has the organization addressed the retention of e-mail messages, voice-mail message, instant messages and other electronic communication tools?

9. Are retention times binding policy, recommendations, guidance, etc.?

10. If the retention times are mandatory, how is compliance verified? (Audits? Written certification? Other?)

11. How does the organization publish or otherwise document retention schedules or communicate them to employees?

12. How does the organization communicate schedules to non-U.S. employees?

13. If the schedules apply globally, how does the organization deal with local requirements?

III. Review how the organization implements retention policy

A. Does the organization provide guidance on:

1. What records are to be created.

2. What format should be used to capture "original" records, status of drafts, working papers and reference copies of records.

B. Evaluate how the organization currently manages the disposal of records

1. Determine to what extent the organization relies on each individual to dispose of/destroy electronic records?

2. How does the organization educate employees about document retention/disposition/destruction responsibilities?

3. How does disposition/destruction occur?

4. What disposal/destruction methods are authorized or required? Is there a difference between paper and electronic?

5. When is information considered "destroyed" within the organization? Is this true for all types/categories of information?

a. When the "delete" button is pushed (*i.e.*, free space pointers are adjusted)

b. When the media has been overwritten? (how many times?)

c. When the media have been physically destroyed?

d. When backups have been overwritten? (how many times?)

e. When an audit log or similar mechanism has been checked, and all copies have been destroyed?

C. Determine if records are being preserved for the required retention period

1. How does the organization ensure that records will remain accessible, readable, and usable throughout their scheduled retention?

2. When records are copied from one medium to another (such as scanning paper records onto optical disk, or microfilming), does the organization retain the originals?

3. Are there appropriate controls in place to address the:

a. life span of the storage medium (*e.g.*, disk or tape decays over time)?

b. obsolescence of software (*e.g.*, moving to a new word processing program)?

c. obsolescence of hardware (*e.g.*, mainframe systems)?

d. obsolescence of the storage medium (*e.g.*, 5.25" disks)?

e. backup media (*e.g.*, tapes) from a records retention perspective?

IV. Evaluate the organization's ability to effectively manage records over their entire lifecycle

A. Estimate records volume

1. Is the volume of paper records increasing, decreasing or stable?

2. What is the volume of electronic records on the company's systems? What are the anticipated increases over the next 1, 3, 5 years?

3. How is the volume of paper records managed? For example, does the organization use in-house storage centers, commercial third-party records storage facilities or other solutions? Is the same done with historical electronic records? If not, what is done?

B. Evaluate the organization's information services/technology ("IT") function including:

1. All hardware used for organization-wide systems (*i.e.*, mainframes, mini computers, e-mail servers, file servers, fax servers, voice-mail servers?)

2. All operating systems (*e.g.*, Windows NT/2000/XP, Linux, Novell, Unix, proprietary?)

3. All desktop hardware and software, including:

a. office document programs (*e.g.*, word processing, spreadsheet programs)

b. internet browsers

c. electronic mail

d. calendar/scheduling

e. database management programs

f. industry-specific applications

g. finance or accounting systems

h. remote connection applications

i. instant mail or "chat" programs

4. All data storage locations available to users (*e.g.*, local hard drives, network drive locations, removable media, third-party storage locations)

5. All portable hardware and software (*e.g.*, notebook computers, PDA, etc.)

6. All "backup" systems (hardware and software)

    a. For what purpose(s) does the organization keep backup media (*e.g.*, tapes)? (Disaster recovery? To restore individual accounts? As a means to ensure records retention? Other?)

    b. How often are backups made? Are they complete backups or incremental?

    c. What is the length of retention of backup media?

    d. Does disposal occur immediately when the retention expires?

    e. If a backup tape is simply released for reuse, is there a concern over the passage of time before reuse occurs?

    f. Is the backup tape degaussed or otherwise erased as a whole, or simply released for reuse?

7. All electronic data archives

8. All network components and locations (*e.g.*, routers, hubs, firewalls, etc.)

9. All data storage locations outside of the United States

10. All third parties involved in data collection or storage on behalf of the organization

11. If the organization uses file servers, how does the organization assure compliance with retention schedules for:

    a. the records on the server?

    b. backup copies of the server?

12. Does the IT function take ownership of records compliance on file servers, or is this left to the users or others?

13. Does the IT function know all the servers?

14. Does the IT function know what types of records are on each server?

15. If an employee places a record on a server (*e.g.*, a word processing document) and forgets about it, how is compliance with retention policies achieved?

16. Is compliance with retention policies a mandatory deliverable for hardware and software?

17. What tools and automation are employed by the organization to manage documents in general and records in particular (for example, Accutrac, iManage, Hummingbird, IBM)

18. Does the organization have a formal electronic records management system?

19. Has the organization implemented formal technology standards for records management? (ISO 15489, DoD 5015.2, ISO 17799)

20. Does the organization employ automated assigning of metadata for content management or control issues to documents?

21. Does the organization use technology to filter outbound content for loss of intellectual property (for example, Sybari for filtering outbound e-mail and attachments)?

22. Does the organization deploy leveraged Digital Rights Management technology to enforce external parties' copyright and license conditions?

23. If a technology is adopted, and concerns regarding records management implications are identified later, what is the process to address those concerns?

C. Review e-mail management procedures

    1. Are employees allowed/encouraged to store e-mail messages for an extended period? (Not allowed or encouraged not to?)

    2. If messages are stored, does the organization have any guidance on where to store them (*e.g.*, inbox versus personal folders or file server) and how to organize them?

    3. If the e-mail messages contain information which may be needed by others in the organization, how is this addressed?

D. Identify the procedures used in the storage of confidential, privileged or other restricted access records

    1. How does the organization categorize information according to sensitivity?

    2. What information security controls does the organization associate with various types of sensitive information?

    3. To what extent is information labeling automated (for example, based upon metadata)?

    4. How does the organization control information that it does not own, but stores or processes on behalf of other entities?

5. How does the organization control information that it owns, but does not store or process?

6. What is the level of awareness and understanding of the organization's information classification and labeling controls among employees generally?

7. What security controls does the organization require for various degrees of sensitive information?

8. Are any levels of sensitive information prohibited from being stored electronically?

   a. From being transmitted over public networks?

   b. From being sent by facsimile?

   c. When is encryption required?

9. Are there any guidelines regarding the use of cell phones or cordless phones for certain levels of sensitive information?

10. What levels of sensitive information require restricted access to hardware?

11. What levels of sensitive information require audit trails for access?

12. What levels of sensitive information require special hardware?

E. Understand policies or procedures in place to monitor or control the release of technical information outside the company

1. Review any employee training program regarding the release of proprietary information

2. Are there processes to review, monitor or control putting confidential information into external e-mails?

3. Are trade secrets classified in any special way?

4. Is access to trade secret information limited or controlled in any way?

5. Does the organization have a way to identify, track or limit the distribution of information that that is controlled by third party obligations?

6. Does the organization have a way to track and search for obligations listed in corporate secrecy or non-disclosure agreements?

7. Does the organization use identity authentication technology (prompt for a specific person's name in a conference call, NetMeeting user identification, etc.)?

The Sedona Guidelines September 2005

V. Evaluate the overall records program

A. With regard to the current records management function, determine the following:

1. How is it organized?

2. How many employees are in the records management function?

3. What other human resources are utilized?

4. How long has it been in existence?

5. Who is in charge?

6. Is the records management function involved in decisions regarding the selection of emerging technologies and new hardware and software? (PDAs, Blackberry®, voice-mail, instant messaging, e-mail systems, enterprise business systems, etc.)

B. Evaluate the existing training/education of employees regarding records management

1. How does the company educate, inform or train employees with respect to their responsibilities for records management?

2. What is the current level of awareness of employees?

C. Review records management compliance methods

1. How does the organization encourage compliance with the records management program's policies and procedures?

2. How does the organization verify compliance?

3. How does the organization staff for compliance overseas?

4. How does the organization verify compliance overseas?

D. Review methods used to manage the records left by employee termination or transfer

1. What is the process for ensuring compliance with records management policies or guidelines when an employee changes job/role or leaves employment with the company?

2. Does this include electronic records such as e-mail, files on servers, etc.?

E. Evaluate the organization's historical records audits practices

1. Does the company have an audit program for records management?

wgs

The Sedona Guidelines *September 2005*

2. What are the purposes of the audits?

3. What types of audits occur? (*e.g.*, individual offices? large paper or electronic systems? other?)

4. Who conducts audits?

5. How are the auditors trained?

6. Approximately what is the volume of auditing that occurs?

F. Evaluate how merger and acquisition (M&A) and divestiture activity have affected the records management program

1. Does the M&A/divestiture transaction result in special agreements about retention?

2. What is the normal expectation about retaining, or not retaining, the records of businesses or subsidiaries that the company divests?

3. Are new subsidiaries or acquired entities expected to follow the records management program? How quickly?

4. If records become "orphaned" as a result of M&A/divestiture activity (*i.e.*, no owner can be identified, and the contents are unknown), what is the process to address this?

VI. Evaluate existing policies regarding litigation or investigations

A. What is the role of the records management function in addressing litigation or investigations?

1. How are documents identified and retrieved? Who is involved?

2. Does the answer differ for paper versus electronic records?

3. If records are located in a company-provided or off-site records storage facility, how are records sorted to identify individual documents that are needed for the litigation or investigation? By whom?

4. When a case is closed, what records are retained and what records are disposed of?

5. If some records are retained after the case is closed, how long are they retained?

6. If you need to halt the disposal of records, how is this accomplished?

7. Has the company issued any guidance for attorneys to promote uniformity?

8. Who is responsible for determining when a suspension is necessary? To write the instruction to suspend disposal? To approve or authorize the suspension? To communicate the suspension of disposal?

9. How is the suspension communicated?

10. How is the suspension worded to make it understandable?

11. How long does it take to develop and issue an instruction to hold records?

12. What principles govern decisions as to the scope (years and varieties) of records that must be held?

13. Are suspended records held in the normal work area or sent elsewhere?

14. When the suspension ends and normal disposal can resume, how is that communicated? How is compliance with the suspension verified?

Once completed, the survey data can be used to develop a new or updated information and records management policy that addresses the specific needs of the organization. The survey results are also likely to identify those areas of the organization where gaps exist between current record-keeping methods and records management best practices.

Resolving these gaps usually requires the development of supporting procedures, guidelines and directives to address specific records life cycle matters. It will also require technological initiatives to incorporate records management requirements into existing and planned business systems. An action plan that prioritizes these additional activities should be developed so that improvements in record-keeping practices address those shortfalls that expose the organization to unnecessary legal or operational risks.

Appendix E: Technical Appendix

This technical appendix is included to provide an extended description and discussion of two important concepts: (1) metadata and (2) electronic (digital) archives.

1. Metadata:

What it is: Metadata (data about data) includes all the contextual, processing, and use information needed to identify and certify the scope, authenticity, and integrity of active or archival electronic information or records. Metadata can come from a variety of sources. It can be created automatically by a computer, supplied by a user, or inferred through a relationship to another document. Metadata is created, modified and disposed of at many points during the life of electronic information or records.[1]

Some metadata, such as file dates and sizes, can easily be seen by users; other metadata may be hidden or embedded and unavailable to computer users who are not technically adept. Metadata is generally not reproduced in full form when a document is printed.

What it does: Metadata may connect to electronic information or records in a variety of ways. The electronic information or record may contain a reference to the metadata, or vice versa. For example, a hypertext document may contain a link to an index that provides information about its context. A folder or directory listing may contain a reference to the location where the content of the electronic document is found.

Why it may be important: Certain metadata is critical in information management and for ensuring effective retrieval and accountability in record-keeping. Metadata can assist in proving the authenticity of the content of electronic documents, as well as establish the context of the content. Metadata can also identify and exploit the structural relationships that exist between and within electronic documents, such as versions and drafts. Metadata allows organizations to track the many layers of rights and reproduction information that exist for records and their multiple versions. Metadata may also document other legal or security requirements that have been imposed on records; for example, privacy concerns, privileged communications or work product, or proprietary interests.

Metadata's importance in searching: Searching capabilities can be significantly enhanced through the existence of rich, consistent metadata. Searching is generally used in records management to select and/or classify data. For example, proper searching can help with the assignment of electronic documents, files and messages into appropriate records management categories. Metadata such as dates, folder information, subject designations and other properties can help generate or validate classifications of the item. Metadata such as e-mail thread information can be used to help assure that related items are maintained in context and/or treated consistently. If descriptive metadata are the same or can be mapped across different electronic repositories, metadata can also make it possible to search across multiple collections or to create virtual collections from materials that are distributed across repositories.

1 Examples of metadata (for electronic document files) include: a file's name, a file's location (*e.g.*, directory structure or pathname), file format or file type, file size, file dates (*e.g.*, creation date, date of last data modification, date of last data access, date of last metadata modification), file permissions (*e.g.*, who can read the data, who can write to it, who can run it). Metadata can also include user-input attributes, such as e-mail subject and addressing, keywords, content description, business purpose, and retention codes and classifications, and the person responsible for the record's retention and disposition.

Metadata and records management: Metadata can also play a crucial role in record lifecycle management. Organizations can design systems that will allow users to input information regarding retention periods and automatically identify or dispose of obsolete records based on those retention periods.

Where it resides: Some metadata is held in structures separate from the core electronic information or record, such as directories, listings and indexes of the files or messages, but may still be regarded as an integral part of the electronic information or record for certain purposes. For example, e-mail messages may be stored with a variety of metadata that may not be viewed by the end-user in the standard setup of the program used to view messages. This metadata may provide important information about a message, such as message thread information that may provide context for the message and a variety of date/time settings. A database may contain metadata, such as the time of entry or modification, the identity of the record's creator, and other information. Document management systems, which are programs designed particularly to preserve tracking and identifying information about electronic documents, hold a great deal of metadata.

The forms it takes: Metadata may be different depending on how or when it is accessed or viewed. For example, when a message is transmitted through an e-mail system it carries with it a variety of metadata, such as the date of creation, transmission to the recipient, and receipt, and the identity of all recipients, including those sent blind carbon copies. After the message has been stored by the recipient, "bcc" information may no longer be directly available to him or her. Yet, when the message is stored by the recipient, "storage level" metadata, not available while the same message is in transmission, may become associated with it. Such storage level metadata may include the folder in which the message is stored and the dates and times it has been re-forwarded or replied to by the recipient.

Metadata migration: For records to remain accessible and intelligible over time, it may be necessary to preserve and migrate the metadata associated with those records. If records that are currently being created are to have a chance of surviving migrations through successive generations of computer hardware and software, or removal to entirely new delivery systems, they will need to have metadata that enables them to exist independently of the system that currently being used to store and retrieve them. Technical, descriptive and preservation metadata that documents how a record was created and maintained, how it behaves and how it relates to other records will all be essential.

Metadata considerations: There will always be important tradeoffs between the costs of developing and managing metadata to meet current needs, and creating sufficient metadata that can be capitalized upon for future, often unanticipated uses. As organizations develop records systems, they should consider which aspects of metadata are essential for what they wish to achieve and how detailed they need each type of metadata to be. An organization may require frequent ad-hoc discovery searches across information systems, protection from inadvertent destruction of documents or e-mail messages, or it may need to prevent disclosure of sensitive trade secrets from being re-distributed or copied.

It should be noted that some software applications carry forward the original author's name in the metadata. Thus, if another person, in creating a new record (*e.g.*, a letter), copies it and then modifies it with new information, it may still reflect the name of the original creator of the record used to recreate the format in the metadata of the new record. In such case, the metadata for the new record may be misleading as to the "real" author of the new record.

Metadata standards: National and international guidelines (such as DoD 5015.2, ISO 15849, Model Requirements for The Management of Electronic Records (MoReq), or ISO 23950 (formerly Z39.50))

can be extremely helpful in making sure that an organization's metadata standards meet the needs of the organization's users.

Transmission of metadata: Individuals who create and transmit electronic documents are often unaware of the existence of readable metadata that may inadvertently reveal privileged or confidential information to adversaries and other outside parties. Organizations should consider adopting policies to provide guidance to users regarding the transmission of metadata. Moreover, many organizations publishing data on "nets" (extra, intra, inter) may not be fully aware of the metadata that may be indexed by outside search engines and viewed by individuals outside the organization.

There are a variety of methods for managing and controlling the extent of metadata transmitted with the core data. Some formats designed for transmission of data, such as XML, provide the functionality for the organization to determine which metadata fields are and are not transmitted with the core data. Other formats, such as the Adobe Portable Document Format (PDF) or Tagged Image Format (TIFF), can be used to remove certain metadata from the core document and to standardize the manner in which the document is maintained. Yet another approach is the use of "metadata stripper" technology, which removes some or all of the metadata from a native electronic file; however, such technology is not available for all types of data and may not be easily usable by end-users. Other technologies may be available for these purposes. Each technology embodies a different approach to the storage and transmission of the core document and metadata, and each may be appropriate in a given set of circumstances, depending on a variety of considerations, including usability of the data, cost, governmental rules and regulations, and other factors.

Metadata and new technology challenges: Emerging technologies may make the management of metadata in the electronic records context much more difficult. For example, "virtual foldering" may allow users to apply several different sets of metadata to a given electronic document depending on the context in which the document is viewed or processed. The metadata in this scenario may not be associated with a single document, but shared across a set of documents through a non document information stores. As technology advances, metadata continues to evolve.

Some types of metadata continue to undergo changes that may increase the difficulty of electronic records management and production of electronic documents for legal proceedings. For example, on some (but not all) existing systems, the user or system administrator can control access to and usage of files and messages by rights or permissions. These constraints can themselves be important metadata properties for legal or records management purposes, and can also impact an organization's ability to store or review its own data. In order to assure that all data can be accessed for purposes of the legal or records management function, permissions or rights to the data must be taken into consideration. Likewise, the legal and records management functions can be affected by encryption of data, procedures for compression and encoding, and other technologies that can make data difficult to identify or review.

One emerging technology that may have a significant impact is known as "electronic rights," which refers to increased control over data access, storage and copying to prevent unauthorized use, primarily in the copyright-protection area. Technologies designed to enforce electronic rights may cause records to be automatically soft-deleted prior to the expiration of its appropriate retention period, or may prevent the record from being reviewed or copied where necessary for records management or litigation purposes. Particularly in the area of audio-visual files (including voice-mail and video recordings) the potential for restrictions in this area are significant.

2. Electronic (Digital) Archives:

What they are: Electronic archives are repositories for electronic records in a form that facilitates searching, reporting, analysis, production, preservation and disposition. When properly set up and maintained, electronic archives are not solely static collections of records (whether on-line or off-line on mass media such as tapes or optical media).

The importance of metadata in electronic archives: The key to maximizing the utility of an electronic archive is the availability of record metadata--especially metadata that cannot be easily derived from the record content--and record management data (such as the business owner, the planned disposition date, various retention factors, etc.) along with the native record. This additional data may add value for searching, reporting and analysis purposes. By adding value for business or user processes, electronic archive systems can present a positive situation for all parties within an organization.

Policies for access to long-term electronic archives should consider requirements for current and post-disposition access to metadata and statistical information.

Long-term business needs for metadata should be weighed against risk and record management requirements for comprehensive removal of both records and their associated metadata at the planned disposition point. These long-term needs may include compliance reporting, productivity analysis, project task and cost analysis, and other forms of detailed and statistical reporting.

Forms of electronic archives: Archives may be monolithic systems encompassing all functions required to create, retrieve, update, and delete electronic records across an organization, or they may be made up of multiple integrated electronic systems. This latter architecture is particularly appropriate for large organizations which already have document management or knowledge management ("KM") systems in place.

Integration of DM/KM and RM: The European Communities' "Model Requirements for the Management of Electronic Records"[2] ("MoReq") distinguishes between a document management ("DM") and records management ("RM") system (equivalent to an electronic archive in this context) as follows:

DM System …	RM System …
Allows documents to be modified and/or to exist in several versions.	Prevents records from being modified.
May allow documents to be deleted by their owners.	Prevents records from being deleted except in certain strictly controlled circumstances.
May include some retention controls.	Must include rigorous retention controls.
May include a document storage structure, which may be under the control of users.	Must include a rigorous record arrangement structure (the classification scheme) which is maintained by the Administrator.
Is intended primarily to support day-to-day use of documents for business.	May support day-to-day working, but is also intended to provide a secure repository for meaningful business records.

2 *Available at* http://www.cornwell.co.uk/moreq.html.

The Sedona Guidelines *September 2005*

Many DM/KM systems contain electronic archive (or electronic records management) functions, either as part of the base system, as add-on components or are available through programmatic features. Where those functions do not exist for the system, it may be necessary to integrate stand-alone DM/KM and electronic archive systems by means of a real-time or periodic transfer between the respective repositories. The development effort involved in this integration can be significant. Both the MoReq and DoD 5015.2-STD[3] provide useful starting points for defining integration requirements.

Electronic archives and e-mail: For most organizations, the ability of the electronic archive to work with existing e-mail systems will be critical. As noted by one publication:

> … the management of e-mail is sometimes characterized as the single biggest records management problem in the USA. Thus, for any organization looking to implement major initiatives in the management of its electronic records, e-mail systems should be the initial focus of such efforts.[4]

Integration of e-mail can vary from simple journaling (also called "logging") of all messages to the electronic archive, to interactive interfacing with the client e-mail application (for example, adding record classification functions to Microsoft Outlook). At a minimum, electronic archives should be able to serve as a repository for e-mail records exported from the e-mail servers. Many commercial e-mail archive and records management add-on products are available for popular e-mail systems (such as Microsoft Exchange and IBM/Lotus Notes).

Electronic archives and technology changes: As new applications are developed or acquired within organizations, the records management requirements relative to those applications should be anticipated and planned as part of the system development or software and/or hardware selection. Digital preservation requires routine efforts to migrate records to overcome software and technological obsolescence and from deteriorating media.

Standards for electronic archives: Long-term electronic archive designs should consider incorporation of national or international specifications such as MoReq or Open Archival Information System (OAIS). Standards such as ISO 15489[5] establish guidelines for records management policies and systems but generally fall short of specifying functional details of automated systems. However, DoD 5015.2 STD and MoReq each contain useful information defining functional requirements for electronic record archives. Both of these also define selected metadata elements required for an electronic records archive. Either document would be appropriate as a starting point for acquisition or construction of an electronic archive system. Finally, both ARMA International and the National Archives Records Administration (NARA) provide planning and guideline documents at their respective web sites.[6]

Tracking non-electronic records: Organizations designing comprehensive long-term electronic archives should consider the need for managing and tracking electronic and non-electronic records. This may include migration from legacy systems tracking paper, film/fiche, artifacts and electronic records.

3 Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (2002), *Design Criteria Standard for Electronic Records Management Software Applications* (DoD 5015.2 STD).
4 David Stephens and Roderick Wallace, *Electronic Records Retention: New Strategies for Data Life Cycle Management* (ARMA International 2003).
5 *Available at* http://www.iso.org. The two components of the standard are ISO 15489-1:2001 and ISO/TR 15489-2:2001.
6 *Available at* http://www.arma.org; *available at* http://www.archives.gov.

Electronic archives and storage media: Policies for maintenance of long-term electronic archives should address selection of storage media and formats appropriate for data usage requirements and planned retention periods, including multi-format and multi-media transfers over the life of records. For the purposes of this discussion, "storage media" refers to the physical devices holding records. For electronic records this is typically fixed or removable hard disks, diskette cartridges ("floppy diskettes" of various sizes, high-density cartridge disks such as those manufactured by Iomega ("Zip disks" and "Jaz disks") and Syquest), optical disks such as CDs and DVDs, or reel and cartridge tape. Excluding the optical disks, all these media store data electromagnetically and are capable of both reading and writing data through many "store-delete-write" cycles. Optical disks, as the name implies, store data by modifying the optical characteristics of a coated plastic disk. Some types of optical disks are capable of both reading and writing through many cycles; others are "Write Once, Read Many" (WORM)—meaning data can be written to the disk only once (that is, it is not updateable) but the disk can be read many times. The most common type of WORM disks are "CD-R" ("Compact Disk-Recordable").

Storage media can be proprietary (controlled by a single corporation, often with details of the construction not available to other parties) or non-proprietary (typically controlled by a standards organization or a consortium of corporations; details of the construction may be available to other parties or restricted to members of the consortium). All present high-density cartridge disks and some forms of cartridge tapes are proprietary designs.

Significant issues may exist with media volume when used for archive purposes. At present, the highest density optical disks offer roughly 10% of the capacity of the highest density magnetic tape cartridges. Physical storage space requirements are comparable between the two (the amount of physical space required to store a given set of data) and storage arrays ("libraries" of multiple optical disks or cartridge tapes) exist for both media. Magnetic cartridge tape remains significantly more common for large-scale and long-term off-line and near-line storage in the corporate community.

When speaking of storage devices, the physical device is only half of the picture. The other half concerns how data records are stored on the physical device. "Format" refers to the binary representation of the data comprising a record. For electronic records there is usually a "native" format: the binary representation used by the application which normally creates, reads, and modifies the record as it is used during the active portion of its lifecycle. As an example, a project status report may be a Microsoft Excel spreadsheet; its format would be the proprietary binary format used by Microsoft for writing of this spreadsheet to storage media (informally this particular format is often called an "XLS file" because of the default file naming ("MyReport.XLS", "Report701.XLS", etc.) used by the Excel program). This format is called a proprietary format because its structure is "owned" and controlled by one corporation (Microsoft in this case). "Non-proprietary" formats may be public domain or made freely available for use by any organization. Some non-proprietary formats are nationally or internationally standardized. For example, the ASCII (American National Standard for Information Interchange) text representation coding is a North American standard. Others are de facto standards, an example of which is the PDF (Portable Document Format) binary representation for documents; this format is widely used by many Internet systems and document management applications.[7]

7 PDF is copyrighted by Adobe Corporation but the specification has been made available for use by any party wanting to read or write documents using this format. Commercial applications writing this format may require a license from Adobe.

wgs™

Ideally, long-term storage formats should be non-proprietary to avoid issues with technological and business obsolescence. However, in practice, non-proprietary formats may not support content and metadata information with sufficient fidelity to serve for archival purposes.

A well-designed electronic archive should support multiple storage media and provide mechanisms for tracking physical write date and time stamps for a given record (that is, the system should track when a record was stored on a given media—this is significantly different from the record creation metadata tracking when a record's content was initially produced).

For records with long retention requirements it may be necessary to copy records to fresh media periodically. This process of copying to new media is referred to as "refreshing." When should refreshed copies be made? The National Library of Australia has concluded the best choices for long-term (over ten year) archival media and format are CD-R media and XML data formatting.[8] Regarding optical media, they note "the lifetime of optical disks of all kinds, and especially CD Rs, is greater than the technological obsolescence factor of their recording and playback technology."[9] NARA, in combination with the National Institute of Standards and Technology (NIST), provides guidance on CD and DVD media and formats in the NIST Special Publication 500-252, *Care and Handling of CDs and DVDs—A Guide for Librarians and Archivists* (NIST October 2003). The results of NIST's evaluations are controversial and do not agree with manufacturer and independent testing.[10] Given the significant variance among these expected life figures, a reasonable compromise may be to use the best quality media available, maintain both on-line and off-line media in an environmentally controlled space (stability appears more important than specific temperature and humidity values), and plan on refreshing copies at intervals of no more than ten years.

Due to rapid technological obsolescence, organizations may wish to consider duplicating particularly valuable records that must be kept for more that ten years to non-electronic media (*e.g.*, computer and output microfilm or "COM;" or archival paper).

Electronic archives and obsolescence: The electronic archive itself may be an application or set of applications. Over time these may change or become obsolete—often in less time than the longest retention period for the records associated with the system. For this reason, the archive architecture must anticipate and support future migration needs to new versions of the archive and the underlying storage media and formats.

Electronic archives and records destruction: Policies for maintenance of long-term electronic archives should address destruction and removal of records (and, as appropriate, their metadata) including any need for forensic-level electronic deletions. Methods for obtaining approval for destruction should be incorporated in the archive system.

Deletion of electronic records has a number of potential issues. In many electronic systems, there are two types of deletion: "logical" (or "soft") deletions which mark record content as being unavailable (but do

8 XML--Extensible Markup Language is a WWW (W3) Consortium standard; XML documents are encoded in UNICODE (itself an ISO standard for international character representations). Conceptually XML documents can contain any type of data (text, multimedia, numeric, etc.). In practice, XML documents are best suited for text and numeric information.

9 Ross Harvey, Presentation at the 2nd Nat'l Preservation Office Conference: Multimedia Preservation--Capturing the Rainbow in Brisbane (Nov. 28 30, 1995), *available at* http://www.nla.gov.au/niac/meetings/npo95rh.html.

10 A recent independent test on CD-R media concluded that many brands of inexpensive optical media have a useful life of less than two years. This contrasts dramatically with the NARA/NIST finding of an expected minimum useful life of 57 years. Refer to *PC-Active* (September 2003) for the most recent documented independent tests (*available at* http://www.aktu.nl/pc-active/cdr.htm (Dutch)); *see Development of a Testing Methodology to Predict Optical Disk Life Expectancy Values* (NIST 500-200), *available at* http://palimpsest.stanford.edu/byorg/nara/nistsum.html; last updated March 2002.

not immediately remove the record metadata or content) and "physical" deletions which remove a record's content from its associated storage media (but do not necessarily remove all record metadata). Physical deletions typically require more time and computing resources than logical deletions. For this reason, physical deletions are often deprecated for systems requiring a high degree of user interactivity. Physical deletions may often be recovered; to prevent such recovery it is necessary to use a "wiping" technology that overwrites the deleted information in such a manner that it would require unusual (and expensive) techniques to accomplish recovery.

Deletion occurs in several levels on modern computer systems:

(a) **File level deletion:** Deletion on the file level renders the file inaccessible to the operating system and normal application programs and marks the space occupied by the file's directory entry and contents as free space, available to reuse for data storage.

(b) **Record level deletion:** Deletion on the record level occurs when a data structure, like a database table, contains multiple records; deletion at this level renders the record inaccessible to the database management system (DBMS) and usually marks the space occupied by the record as available for reuse by the DBMS, although in some cases the space is never reused until the database is compacted. Record level deletion is also characteristic of many e-mail systems.

(c) **Byte level deletion:** Deletion at the byte level occurs when text or other information is deleted from the file content (such as the deletion of text from a word processing file); such deletion may render the deleted data inaccessible to the application intended to be used in processing the file, but may not actually remove the data from the file's content until a process such as compaction or rewriting of the file causes the deleted data to be overwritten.

Electronic archives should provide disposition functions for both logical and physical record deletions and permit specification of which, if any, associated metadata elements should be removed.

One issue that often arises is tracking details of when and how a given record may have been removed from the archive. In the paper world, "Certificates of Destruction" exist as proof that a set of records was destroyed by a particular method and by a specific organization on a given date. If a need exists for similar compliance documentation on electronic records, it will be necessary to keep a minimal set of metadata about those records to have a "target" for the data tracking the disposition. This requirement will only exist if it is necessary to track the disposition information on specific records. Generic statistics (for example, a count of records deleted) can be maintained without retaining record metadata.

Electronic archives and security: Policies for access to long-term electronic archives should consider requirements for ownership and control including, but not limited to, security, traceability, authenticity, and change-control over the record lifecycle.

The National Archives and Records Administration (NARA) *Concept of Operations* provides useful guidelines for typical user functions and associated ownership concerns:

Access—all consumers will be able to search and retrieve descriptions of records accessioned by NARA. In addition, they will be able to search and retrieve electronic records which have no access restrictions that are maintained in [electronic records archive ("ERA")]. Consumers with

special access rights (clearances) and privileges may check those clearances with ERA upon accessing the system.

Search—the consumer searches ERA for information describing electronic records and for actual content within electronic records. Such searching may be done at a variety of levels of aggregation (*i.e.*, record group or set, series, file unit, or item). Within the consumer's given access rights and privileges, the consumer may take advantage of available functions and features. ERA responds to search queries against descriptions by supplying the descriptions that match search criteria. Normally, records are described at the set level, such as series or file unit. If records lifecycle data identifies a group of electronic records of interest, the consumer may proceed to run queries against the content of those records of interest, the consumer may proceed to run queries against the content of those records. ERA responds to search queries by identifying either sets of electronic records, or individual electronic records, with results constrained by the consumer's access rights. ERA provides the capability for the consumer to view and/or sort the results of the search, modify the search if necessary, and refine or save search results as desired. The consumer is able to perform these functions in an iterative manner, thus permitting the user to progress from a search about a general topic to a list of specific electronic records that the consumer may wish to view.

Retrieve/Receive—from search results that identify relevant electronic records, ERA allows the consumer to view and access the electronic records desired. The consumer directly interacts with the ERA system and accesses records in accordance with established privileges and access rights. The consumer may request the ERA system to output electronic records to a selected medium or print them in formats with parameters chosen from available options. ERA also provides the capability to direct output via telecommunications, for example, using File Transfer Protocol (FTP). The consumer may use search and retrieval capabilities without any involvement of NARA staff, but if at any time the consumer has questions, has trouble searching, requires services, or is unable to retrieve/receive records due to access restrictions, ERA provides the consumer the capability to request a mediated search.[11]

User roles for electronic archives: When planning for specific control over the access, search, and retrieval rights of records in an archive there are a number of possible user roles. Users serving in these roles work in different ways—and at different times in the record lifecycle—with the archive itself, the record content and metadata, and the records policy infrastructure. Within the electronic archive there may be specific metadata associated with each role. The NARA *Concept of Operations* guide provides a working set of typical roles:

Transferring Entity [may also be called the "Author" or "User" in some contexts]—makes or receives records, prepares and transfers them to NARA. This class of users primarily consists of records creators, but the name was chosen to indicate the predominate interaction with the system;

11 *Electronic Records Archives Concept of Operations* (CONOPS v. 4.0) Section 6.6.2 (Consumer Activities); National Archives and Records Administration Electronic Records Archives Program Management Office, July 27, 2004, *available at* http://www.archives.gov/era/pdf/concept-of-operations.pdf. Note that this section defines additional classes of activities, specifically "Mediated Request" and "Fee for Service" functions, which do not apply in typical corporate archive environments.

Appraiser—assesses the records with respect to informational value, artifactual value, evidential value, associational value, administrative value, and monetary value and recommends which records should be accessioned into NARA's assets and which should be disposed of by the Transferring Entity when no longer needed by the Transferring Entity;

Record Processor—manages transfers of records, identifies arrangements and creates archival description of records, carries out other processes needed to ensure the availability of records, is responsible for the disposal of temporary records;

Preserver—plans the system approach for maintaining the authentic context, content, and structure of electronic records over time for viewing, use, and downloading. Concisely, the preserver plans processing activities that ensure ability to provide long-term access to electronic records through implementation of the Preservation and Access Plan;

Access Reviewer—reviews security classified or otherwise potentially access restricted information in order to determine if the information can be made available to a consumer, facilitating redaction of potentially access restricted information in electronic records. The Access Reviewer reviews records in NARA custody and sets access restrictions;

Consumer—uses the system to search for and access records, to submit FOIA requests, request assistance via mediated searches, communicate with NARA, and invoke system services;

Administrative User—directly supports the overall operations and integrity of ERA and its use, and manages such system activities as user rights, monitoring system performance, and scheduling reports; and

NARA Manager—reviews system recommendations and makes decisions on when and how specific records lifecycle activities occur, and who will perform the work. The manager has ultimate responsibility for the completion of tasks and the quality of the products.[12]

This set should not be taken as absolute: many organizations will have only some of the roles, and some organizations will have additional roles. In particular, records management policies may define other roles (such as "Official Record Owner", "Records Contact", etc.) as appropriate for a given environment and organizational context. Finally, for electronic archives some roles, such as "Record Processor" may be handled by automated agents (that is, by software rather than people).

There are additional Information Technology or Services (IT/IS) roles that may apply to an electronic archive system. These roles would be responsible for the creation and maintenance of the application software, hardware, and underlying database technology.

12 *Electronic Records Archives Concept of Operations* (CONOPS v. 4.0) Section 5.5 (User Classes and Other Involved Personnel); National Archives and Records Administration Electronic Records Archives Program Management Office, July 27, 2004, *available at* http://www.archives.gov/era/pdf/concept-of-questions.pdf.12

User management to control and track access, as well as change ownership and user roles, should be handled by an archive administration role. The NARA *Concept of Operations* guide refers to this role as the "administrative user" and describes three activities associated with the role:[13]

> **User rights and privileges**—the administrative user assigns user rights and privileges based upon clearances held, permissions granted, job roles captured at the time of registration within the system, and RM policy.
>
> **Schedule Reports**—the request for reports could be based on a specific requirement from RM policy or from a system monitoring need.
>
> **Monitor System**—the Electronic Records Archive (ERA) provides the administrative user with the ability to monitor system performance and security.

The need for reporting functions: Reporting functions within the electronic archive—or the equivalent facility to report against the data technology underlying the archive (for example, to perform SQL ("Structured Query Language") queries against an Oracle database on which the archive was built)—should provide access to historical, transactional and current record management metadata sufficient for auditing and verification of the archive. These tools provide the mechanisms critical to on-going validation of archive use, policy compliance, litigation analysis and extraction, and statutory or regulatory processing requirements.

13 *Electronic Records Archives Concept of Operations* (CONOPS v. 4.0) Section 4.0 (Administrative User Scenario); National Archives and Records Administration Electronic Records Archives Program Management Office, July 27, 2004, *available at* http://www.archives.gov/era/pdf/concept-of-questions.pdf.

Appendix F: Glossary

This glossary is intended to define terms of art used in this white paper or common to the disciplines of records management and information technology as they relate to topics covered here, including the identification, collection, and analysis of information and records for investigation and litigation. This glossary is not comprehensive or exhaustive of such terms. References to "DoD 5015" refer to Department of Defense "Design Criteria for Electronic Record Management Software Applications" (October 2003). Readers may also wish to consult The Sedona Conference® Glossary for E-Discovery and Digital Information Management (May 2005) available at: www.thesedonaconference.org/content/miscFiles/tsglossarymay05

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

Active Records: Active Records are those records related to current, ongoing or in-process activities and are referred to on a regular basis to respond to day-to-day operational requirements. An active record resides in native application format and is accessible for purposes of business processing with no restrictions on alteration beyond normal business rules. *See* Inactive Records.

Ambient Data: *See* Residual Data.

Application: An application is a collection of one or more related software programs that enables a user to enter, store, view, modify or extract information from files or databases. The term is commonly used in place of "program," or "software." Applications may include word processors, Internet browsing tools and spreadsheets.

Archival Data: Archival Data is information that is not directly accessible to the user of a computer system but that an organization maintains for long-term storage and record-keeping purposes. Archival data may be written to removable media such as a CD, magneto-optical media, tape or other electronic storage device, or may be maintained on system hard drives or network servers. (This term, unlike the following term, is derived from IT vocabulary.)

Archive, Electronic Archive: Archives are long term repositories for the storage of records. Electronic archives preserve the content, prevent or track alterations and control access to electronic records. *See* the discussion of electronic archives in the Technical Appendix, Appendix E. (This term, unlike the preceding term, is derived from records management vocabulary.)

Attachment: An attachment is a record or file associated with another record for the purpose of storage or transfer. There may be multiple attachments associated with a single "parent" or "master" record. The attachments and associated record may be managed and processed as a single unit. In common use, this term refers to a file (or files) associated with an e-mail for transfer and storage as a single message unit. Because in certain circumstances the context of the attachment--for example, the parent e-mail and its associated metadata--can be important, an organization should consider whether its policy should authorize or restrict the disassociation of attachments from their parent records.

Attribute: An attribute is a characteristic of data that sets it apart from other data, such as location, length, or type. The term attribute is sometimes used synonymously with "data element" or "property."

Author or Originator: The author of a document is the person, office or designated position responsible for its creation or issuance. In the case of a document in the form of a letter, the author or originator is usually indicated on the letterhead or by signature. In some cases, the software application producing the document may capture the author's identity and associate it with the document. For records management purposes, the author or originator may be designated as a person, official title, office symbol or code. (DoD 5015)

Backup Data: Backup Data is information that is not presently in use by an organization and is routinely stored separately upon portable media. Backup data serves as a source for recovery in the event of a system problem or disaster. Backup data is distinct from "Archival Data."

Backup Tape Recycling: Backup Tape Recycling describes the process whereby an organization's backup tapes are overwritten with new data, usually on a fixed schedule determined jointly by records management, legal and IT sources. For example, the use of nightly backup tapes for each day of the week with the daily backup tape for a particular day being overwritten on the same day the following week; weekly and monthly backups being stored offsite for a specified period of time before being placed back in the rotation.

Backup tapes: *See* Disaster Recovery Tapes.

Compact Disk (CD): A type of optical disk storage media, compact disks come in a variety of formats. These formats include CD-ROMs ("CD-Read-Only-Memory") that are read-only; CD-Rs ("CD-Recordable") that are write to once and are then read only; and CD-RWs (CD-Read-Write") that are write to in multiple sessions.

Computer Forensics: Computer Forensics (in the context of this document, "forensic analysis") is the use of specialized techniques for recovery, authentication and analysis of electronic data when an investigation or litigation involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data by technical analysis or explanation of technical features of data and computer usage. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel, and generally requires strict adherence to chain-of-custody protocols.

Custodian: *See* Record Custodian.

Data Element: A combination of characters or bytes referring to one separate piece of information, such as name, address, or age. (DoD 5015)

Database Management System (DBMS): A software system used to access and retrieve data stored in a database. (DoD 5015)

Database: In electronic records, a set of data elements, consisting of at least one file or of a group of integrated files, usually stored in one location and made available to several users. (DoD 5015)

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

Delete, Deletion: The process of permanently removing, erasing or obliterating recorded information from a medium, especially a reusable magnetic disk or tape. (DoD 5015) Deletion is the process whereby data is removed from active files and other data storage structures on computers and rendered inaccessible except by using special data recovery tools designed to recover deleted data.

Deleted Data: Deleted Data are data that existed on the computer as live data and which have been deleted by the computer system or end-user activity. Deleted data may remain on storage media in whole or in part until they are overwritten or "wiped." Even after the data have been wiped, directory entries, pointers or other information relating to the deleted data may remain on the computer. "Soft deletions" are data marked as deleted (and not generally available to the end-user after such marking), but not yet physically removed or overwritten. Soft-deleted data can be restored with complete fidelity.

Disaster Recovery Tapes: Disaster Recovery Tapes are portable media used to store data for backup purposes. *See* Backup Data.

Disposition: The final business action carried out on a record. This action generally is to destroy or archive the record. Electronic record disposition can include "soft deletions" (*see* Deletion), "hard deletions," "hard deletions with overwrites," "archive to long-term store," "forward to organization," and "copy to another media or format and delete (hard or soft)."

Distributed Data: Distributed Data is that information belonging to an organization which resides on portable media and non-local devices such as remote offices, home computers, laptop computers, personal electronic assistants ("PDAs"), wireless communication devices (*e.g.*, Blackberry), internet repositories (including e-mail hosted by internet service providers or portals and web sites) and the like. Distributed data also includes data held by third parties such as application service providers and business partners. In the event of litigation, distributed data may present additional issues for collection and analysis. *Note*: Information Technology organizations may define distributed data differently (for example, in some organizations distributed data includes any non-server-based data, including workstation disk drives).

Draft Record: Draft records can include working files such as preliminary drafts, notes, supporting source documents and similar materials. Organizations may determine that drafts should be retained if (1) they contain unique information including the substantive mental impressions of the author as to a business policy, decision, action or responsibility; or (2) they reflect substantive comments, annotations or comments by persons other than the author concerning a business policy, decision, action or responsibility; or (3) they are transmitted, circulated or made available to persons other than the author for business purposes such as approval, comment, action, recommendation or follow-up.

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

Electronic Mail Message: A document created or received via an electronic mail system, including brief notes, formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message. 36 C.F.R. § 1234.2, reference (aa). (DoD 5015)

Electronic Record: Information recorded in a form that requires a computer or other machine to process it and that otherwise satisfies the definition of a record. (DoD 5015)

File Plan: A document containing the identifying number, title, description and disposition authority of files held or used in an office. (DoD 5015)

Forensic Copy: A forensic copy is an exact copy of the entire physical storage media (hard drive, CD-ROM, DVD-ROM, tape, etc.), including all active and residual data and unallocated space on the media. Forensic copies are often called "image or imaged copies".

Format: The internal structure of a file, which defines the way it is stored and used. Specific applications may define unique formats for their data (*e.g.*, "MS Word document file format"). Many files may only be viewed or printed using their originating application or an application designed to work with compatible formats. Computer storage systems commonly identify files by a naming convention that denotes the format (and therefore the probable originating application)

(*e.g.*, "DOC" for Microsoft Word document files; "XLS" for Microsoft Excel spreadsheet files; "TXT" for text files; and "HTM" (for Hypertext Markup Language (HTML) files such as web pages). Users may choose alternate naming conventions, but this may affect how the files are treated by applications.

Hold: *See* Legal Hold.

Image Copy, Imaged Copy: *See* Forensic Copy.

Inactive Record: Inactive records are those records related to closed, completed, or concluded activities. Inactive records are no longer routinely referenced, but must be retained in order to fulfill reporting requirements or for purposes of audit or analysis. Inactive records generally reside in a long-term storage format remaining accessible for purposes of business processing only with restrictions on alteration. In some business circumstances, inactive records may be re-activated.

Information: For the purposes of this document, information is used to mean both documents and data.

Instant Message, Instant Messaging ("IM"): Instant Messaging is a form of electronic communication, which involves immediate correspondence between two or more users who are all online simultaneously. Some IM communications (peer-to-peer) may not be stored on servers after receipt.

Janitor Program: An application which runs at scheduled intervals to manage business information by deleting, transferring, or archiving on-line data (such as e-mail) at specific points in time. Janitor programs are sometimes referred to as "agents"—software that runs autonomously "behind the scenes" on user systems and servers to carry out business processes according to pre-defined rules.

Legacy Data, Legacy System: Legacy Data is information in which an organization may have invested significant development resources and which has retained its importance but has been created or stored by the use of software and/or hardware that has become obsolete or replaced ("legacy systems"). Legacy data may be costly to restore or reconstruct when required for investigation or litigation analysis or discovery.

Legal Hold: A legal hold is a communication issued as a result of current or anticipated litigation, audit, government investigation or other such matter that suspends the normal disposition or processing of records. The specific communication to business or IT organizations may also be called a "hold," "preservation order," "suspension order," "freeze notice," "hold order," or "hold notice."

Lifecycle: The records lifecycle is the life span of a record from its creation or receipt to its final disposition. It is usually described in three stages: creation, maintenance and use, and archive to final disposition.

Metadata: Metadata is information about a particular data set which describes how, when and by whom it was collected, created, accessed or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information). *See* Technical Appendix E for discussion of Metadata.

Migration: Moving files to another computer application or platform which may require changing their formats.

Mount, Mounting: The process of making off-line data available for on-line processing. For example, placing a magnetic tape in a drive and setting up the software to recognize or read that tape. The terms "load" and "loading" are often used in conjunction with, or synonymously with, "mount" and "mounting" (as in "mount and load a tape"). "Load" may also refer to the process of transferring data from mounted media to another media or to an on-line system.

Native Format: Electronic documents have an associated file structure defined by the original creating application. This file structure is referred to as the "native format" of the document. Because viewing or searching documents in the native format may require the original application (for example, viewing a Microsoft Word document may require the Microsoft Word application), documents are often converted to a vendor-neutral format as part of the record acquisition or archive process. *Cf.* "Static" formats.

Near-line data storage: Storage in a system that is not a direct part of the network in daily use, but that can be accessed through the network. There is usually a small time lag between the request for data stored in near-line media and its being made available to an application or end-user. Making near-line data available will not require human intervention (as opposed to "off-line" data which can only be made available through human actions).

Official Record Owner: *See* Record Owner.

Off-line data: The storage of electronic data outside the network in daily use (*e.g.*, on backup tapes) that is only accessible through the off-line storage system, not the network.

On-line storage: The storage of electronic data as fully accessible information in daily use on the network or elsewhere.

Preservation Notice, Preservation Order: *See* Legal Hold.

Record: Information, regardless of medium or format, that has value to an organization. Collectively the term is used to describe both documents and electronically stored information.

Record Custodian: A records custodian is an individual responsible for the physical storage and protection of records throughout their retention period. In the context of electronic records, custodianship may not be a direct part of the records management function in all organizations. For example, some organizations may place this responsibility within their information technology department, or they may assign responsibility for retaining and preserving records with individual employees. For this reason, this publication discusses the possibility of having a content custodian and a technology custodian.

Record Lifecycle: The time period from when a record is created until it is disposed.

Record Owner: The records owner is the subject matter expert on the content of the record and is responsible for the lifecycle management of the record. This may be, but is not necessarily, the author of the record.

Record Series: A description of a particular set of records within a file plan. Each category has retention and disposition data associated with it, applied to all record folders and records within the category. (DoD 5015)

Records Hold: *See* Legal Hold.

Records Management: Records Management is the planning, controlling, directing, organizing, training, promoting and other managerial activities involving the life-cycle of information, including creation, maintenance (use, storage, retrieval) and disposition, regardless of media.

Records Manager: The records manager is responsible for the implementation of a records management program in keeping with the policies and procedures that govern that program, including the identification, classification, handling and disposition of the organization's records on all media throughout their retention life. The physical storage and protection of records may be a component of this individual's functions, but it may also be delegated to someone else. *See* Records Custodian.

Records Retention Period, Retention Period: The length of time a given records series must be kept, expressed as either a time period (*e.g.*, four years), an event or action (*e.g.*, audit), or a combination (*e.g.*, six months after audit).

Records Retention Schedule: A plan for the management of records, listing types of records and how long they should be kept; the purpose is to provide continuing authority to dispose of or transfer records to historical archives.

Records Store: *See* Repository for Electronic Records.

Record Submitter: The Record Submitter is the person who enters a record in an application or system. This may be, but is not necessarily, the author or the record owner.

Recover, Recovery: *See* Restore.

Report: Formatted output of a system providing specific information.

Repository for Electronic Records: Repository for Electronic Records is a direct access device on which the electronic records and associated metadata are stored. (DoD 5015) Sometimes called a "records store" or "records archive."

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

Restore: To transfer data from a backup medium (such as tapes) to an on-line system, often for the purpose of recovery from a problem, failure, or disaster. Restoration of archival media is the transfer of data from an archival store to an on-line system for the purposes of processing (such as query, analysis, extraction or disposition of that data). Archival restoration of systems may require not only data restoration but also replication of the original hardware and software operating environment. Restoration of systems is often called "recovery".

Retention Schedule: *See* Records Retention Schedule.

Sampling: Sampling usually (but not always) refers to the process of testing a database for the existence or frequency of relevant information. It can be a useful technique in addressing a number of issues relating to litigation, including decisions about what repositories of data are appropriate to search in a particular litigation and determinations of the validity and effectiveness of searches or other data extraction procedures. Sampling can be useful in providing information to the court about the relative cost burden versus benefit of requiring a party to review certain electronic records.

Slack Space: A form of residual data, slack space is the amount of on-disk file space from the end of the logical record information to the end of the physical disk record. Slack space can contain information soft-deleted from the record, information from prior records stored at the same physical location as current records, metadata fragments and other information useful for forensic analysis of computer systems.

Spoliation: Spoliation is the destruction of records which may be relevant to ongoing or anticipated litigation, government investigation or audit. Courts differ in their interpretation of the level of intent required before sanctions may be warranted. *See* Guideline 3.

Static formats: "Static" formats (often called "imaged formats") are designed to retain a "picture" of the document as it would look viewed in the original creating application but do not allow manipulation of the document information; such formats may be well-suited for many records and litigation uses where access to document metadata and preservation of original document structures are not important. *Cf.* Native Formats.

Suspension Notice, Suspension Order: *See* Hold.

System: A system is: (1) a collection of people, machines and methods organized to perform specific functions; (2) an integrated whole composed of diverse, interacting, specialized structures and sub-functions; and/or (3) a group of sub-systems united by some interaction or interdependence, performing many duties but functioning as a single unit.

Version, Record Version: A particular form of or variation from an earlier or original record. For electronic records, the variations may include changes to file format, metadata or content.

Vital Record: A record that is essential to the organization's operation or to the reestablishment of the organization after a disaster.

Web site: A collection of Uniform Resource Indicators (URIs, including URLs (Uniform Resource Locators)) in the control of one administrative entity. May include different types of URIs (*e.g.*, file transfer protocol sites, telnet sites, as well as World Wide Web sites).

Appendix G: Working Group Participants, Members & Observers

As of August 25, 2005

Woods Abbott, Esquire
Raytheon Company
Member

Whitney Adams, Esquire
Cricket Technologies
Member

Sharon A. Alexander, Esquire
Jones Day
Participant

Dr. Jacqueline M. Algon
Participant

Thomas Y. Allman, Esquire
Mayer, Brown, Rowe & Maw LLP
Steering Committee Member

Susan Avery
ARMA International
Participant

Jennifer V. Baker
Navigant Consulting, Inc.
Participant

Thomas I. Barnett, Esquire
Sullivan & Cromwell
Participant

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

Diane Barrasso
Barrasso Consulting LLC
Member

Jim Barrick
CaseCentral
Member

Bobbi Basile
Ernst & Young
Member

Charles A. Beach, Esquire
Exxon Mobil Corporation
Participant

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

Steven C. Bennett, Esquire
Jones Day
Participant

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

Joanna Blackburn CRM
Union Pacific Railroad
Participant

Stephanie A. Blair, Esquire
Morgan Lewis & Bockuis LLP
Participant

Alan F. Blakley, Esquire
Thomas M. Cooley Law School
Member

Hildy Bowbeer, Esquire
3M Company
Member

John J. Bowers, Esquire
Womble Carlyle Sandridge & Rice, PLLC
Member

Kevin F. Brady, Esquire
Connolly Bove Lodge & Hutz LLP
Participant

Richard G. Braman, Esquire
The Sedona Conference
Observer, *ex-officio* Steering Committee Member

Kerry A. Brennan, Esquire
Pillsbury Winthrop Shaw Pittman LLP
Member

Charlene A. Brownlee, Esquire
Fulbright & Jaworski LLP
Member

Colin E. Burdick
Bowne Business Solutions, Inc.
Member

The Sedona Guidelines *September 2005*

Macyl Burke
ACT Litigation Services
Member

Christine M. Burns
Cohasset Associates, Inc.
Participant

Paul E. Burns, Esquire
Steptoe & Johnson, LLP
Member

Karen Buzga
Milberg Weiss Bershad & Schulman LLP
Member

Bridget Calia
ARMA International
Participant

Diane K. Carlisle
Baker Robbins & Company
Participant

The Honorable John L. Carroll (Ret.)
Cumberland School of Law
Observer

Vincent Catanzaro, Esquire
Kelly Law Registry
Member

Barbara A. Caulfield, Esquire
Affymetrix, Inc.
Member

M. Kate Chaffee
Faegre & Benson LLP
Member

Michael A. Clark
EDDix LLC
Participant

R. Noel Clinard, Esquire
Hunton & Williams LLP
Participant

Adam I. Cohen, Esquire
Weil, Gotshal & Manges LLP
Participant

Andrew M. Cohen, Esquire
EMC Corporation
Participant

Matthew Cohen, Esquire
Skadden Arps Slate Meagher & Flom LLP
Participant

Harald Collet
Oracle Corporation
Member

Alfred W. Cortese, Jr., Esquire
Cortese PLLC
Participant

Jim Coulson
Records Improvement Institute LLC
Member

Conor R. Crowley, Esquire
Much, Shelist, Freed, Denenberg, Ament & Rubenstein, PC
Participant

Tim Crouthamel, Esquire
State Farm Insurance Company
Participant

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

Jonathan A. Damon, Esquire
LeBoeuf, Lamb, Greene & MacRae LLP
Participant

Martha J. Dawson, Esquire
Preston, Gates & Ellis, LLP
Participant

Robert J. C. Deane, Esquire
Borden Ladner Gervais LLP
Member

Daniel T. DeFeo, Esquire
The DeFeo Law Firm, PC
Member

Daniel DeJoy
Xerox
Member

John Paul Deley
Energy Information Administration
Observer

Trudy Downs
Merck & Co. Inc.
Member

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

Peg Duncan
Department of Justice, Canada
Observer

wgs

Robert A. Eisenberg, Esquire
DOAR
Participant

Laura E. Ellsworth, Esquire
Jones Day
Participant

Colin C. Elrod
LECG
Member

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

The Hon. John M. Facciola
United States Magistrate Judge
District of Columbia
Observer

Joan E. Feldman
Navigant Consulting, Inc.
Member

Eric R. Finkelman, Esquire
Ciba Specialty Chemicals Corporation
Member

Delilah Flaum, Esquire
Mayer, Brown, Rowe & Maw LLP
Member

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

Jeffrey Fowler, Esquire
O'Melveny & Myers LLP
Member

Craig J. Freeman
Navigant Consulting, Inc.
Member

Thomas Freeman, Esquire
Reed Smith LLP
Member

Suzanne Frost
Faegre & Benson LLP
Member

Thomas E. Gaeta
Navigant Consulting, Inc.
Member

James H. Gallegos, Esquire
Burlington Northern and Santa Fe Railway
Member

Barbara K. Geier, Esquire
King & Spalding LLP
Member

Patrick J. Gennardo, Esquire
LeBoeuf, Lamb, Greene & MacRae LLP
Member

Edward Glynn
PricewaterhouseCoopers LLP
Participant

James E. Gordon
Navigant Consulting, Inc.
Participant

Ross M. Gotler
Paul Weiss Rifkind Wharton & Garrison LLP
Member

David Grant, Esquire
Wal Mart Stores, Inc.
Member

Ronald J. Green
Bank of America
Participant

Brian Hail
Haynes & Boone LLP
Member

Earl Harcrow, Esquire
Haynes and Boone, LLP
Member

Matthew S. Harman, Esquire
King & Spalding LLP
Member

Sherry B. Harris
Hunton & Williams LLP
Participant

Charles Hart
Member

Bruce Hartley
Cricket Technologies
Member

Jeff Hatfield
Jordan Lawrence Group
Member

Kris Haworth
Navigant Consulting, Inc.
Participant

Honorable Ronald J. Hedges
United States Magistrate Judge
District of New Jersey
Observer

Ted S. Hiser, Esquire
Jones Day
Participant

Julie Hoff
Faegre & Benson LLP
Member

Timothy H. Hood
Faegre & Benson LLP
Member

Virginia W. Hoptman, Esquire
Womble Carlyle Sandridge & Rice, PLLC
Member

Karen O. Hourigan, Esquire
Jones Day
Member

Geoffrey M. Howard, Esquire
Bingham McCutchen LLP
Member

David W. Ichel
Simpson Thacher & Bartlett LLP
Member

David K. Isom, Esquire
Greenberg Traurig
Member

Conrad Jacoby, Esquire
Potomac Consulting Group
Participant

John Janes
Deloitte
Member

William R. Jenkins, Jr., Esquire
Jackson Walker, LLP
Member

John H. Jessen
Electronic Evidence Discovery, Inc.
Steering Committee Member

Deborah A. Johnson
National Data Conversion
Participant

Glenn Johnson
King & Spalding LLP
Member

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

Monica Johnson
Faegre & Benson LLP
Member

Jeffrey J. Joyce, Esquire
Jones Day
Participant

Sidney Kanazawa, Esquire
Van Etten Suzumoto & Becket LLP
Participant

Dr. Hironao Kaneko
Tokyo Institute of Technology
Observer

Larry Kanter
Alvarez & Marsal
Member

Gaither Keener, Jr., Esquire
Lowe's Companies, Inc.
Member

Chuck Kellner
Daticon, Inc.
Member

John B. Kennedy, Esquire
LeBoeuf, Lamb, Greene & MacRae LLP
Member

Anne Kershaw, Esquire
A. Kershaw PC, Attorneys & Consultants
Participant

Laura M. Kibbe, Esquire
Pfizer Inc.
Member

Elizabeth Kidd, Esq.
iCite Legal, Division of Aspen Systems
Member

Dennis Kiker
Moran Kiker Brown PC
Participant

Mary Ann Kim
DuPont Company
Participant

Mike Kinnaman
Attenex Corporation
Member

David Kittrell
Participant

Gene Klimov, Esquire
DOAR
Member

Kelly Kruse
Faegre & Benson LLP
Member

James S. Kurz, Esquire
Womble Carlyle Sandridge & Rice, PLLC
Member

Monica W. Latin, Esquire
Carrington Coleman Sloman & Blumenthal
Participant

Brandon Leath
Electronic Evidence Discovery, Inc.
Member

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

Pauline Levy, Esquire
McDonald's Corporation
Member

Robert Levy
Haynes and Boone LLP
Member

Julie Lewis
Digital Mountain, Inc.
Member

Thomas A. Lidbury, Esquire
Mayer, Brown, Rowe & Maw LLP
Member

Steve Lilley
iLumin Software Services, Inc.
Member

Stefanie Lindeman
Faegre & Benson LLP
Member

Amy Jane Longo, Esquire
O'Melveny & Meyers LLP
Member

Joe Looby
FTI Consulting
Participant

Chris Maconi
Electronic Evidence Discovery, Inc.
Member

Sheri Malec
McDonald's Corporation
Member

A. John P. Mancini, Esquire
Mayer, Brown, Rowe & Maw LLP
Participant

David G. Martin, Esquire
Medtronic, Inc.
Participant

Browning E. Marean, III, Esq.
DLA Piper Rudnick Gray Cary US LLP
Member

Geoffrey C. Mason, Esquire
Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
Member

Wayne Matus, Esquire
Mayer, Brown, Rowe & Maw LLP
Participant

Tom Matzen, Esquire
XACT - IDS
Member

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

Gregory McCurdy, Esquire
Microsoft Corp.
Participant

Stephanie Mendelsohn, Esquire
Reed Smith
Participant

Joshua Metzger
X1 Technologies
Member

James L. Michalowicz
Tyco International (US), Inc.
Participant

Bruce Miller
IBM Canada Ltd.
Member

Scott A. Milner, Esquire
Morgan Lewis & Bockius LLP
Member

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

John Montaña, Esquire
Cunningham & Montaña, Inc.
Member

Timothy L. Moorehead, Esquire
BP America, Inc.
Steering Committee Member

Jack Moorman
PricewaterhouseCoopers LLP
Participant

Helen Bergman Moure, Esquire
Preston Gates & Ellis LLP
Participant

Paul J. Neale, Jr.
DOAR
Member

Dana Novak
Faegre & Benson LLP
Member

Jonathan Nystrom
Cataphora
Member

Kate O'Brien
Digital Mandate
Member

Kate Oberlies O'Leary, Esquire
General Electric Company
Participant

Maureen E. O'Neill, Esquire
Paul, Hastings, Janofsky & Walker
Member

Timothy M. Opsitnick, Esquire
JurInnov Ltd.
Participant

Greg Osinoff
Digital Mandate
Member

Robert D. Owen, Esquire
Fulbright & Jaworski, LLP
Member

Laura Lewis Owens, Esquire
Alston & Bird LLP
Participant

Neil Packard
Seltzer Caplan McMahon Vitek
Member

Robert W. Pass, Esquire
Carlton Fields
Participant

John Patzakis
Guidance Software
Member

Richard Pearce-Moses
Director of Digital Government Information
Arizona State Library, Archives and Public Records
Observer

Cheryl L. Pederson, CRM
Cargill Inc.
Member

Peter Pepiton II, Esquire
iLumin Software Services, Inc.
Member

Jeanette Plante
United States Department of Justice
Observer

Vivian Polak, Esquire
LeBoeuf, Lamb, Greene & MacRae LLP
Participant

Ashish S. Prasad, Esquire
Mayer, Brown, Rowe & Maw LLP
Steering Committee Member

Michael J. Prounis
Evidence Exchange
Participant

Charles R. Ragan, Esquire
Pillsbury Winthrop Shaw Pittman LLP
Participant

Jonathan M. Redgrave, Esquire
Jones Day
Steering Committee Chair

Jeffrey Reed
Eckert Seamans Chapin & Mallott LLC
Member

Dan Regard, Esquire
LECG, LLC
Participant

Mark V. Reichenbach
Milberg Weiss Bershad & Schulman LLP
Participant

David Remnitz
FTI Consulting
Participant

Mary K. Riley
Bank of America
Participant

Louise A. Rinn, Esquire
Union Pacific Railroad Company
Participant

Paul M. Robertson, Esquire
Bingham McCutchen LLP
Participant

Steven R. Rodgers
Intel Corporation
Member

Jeff Rodwell, Esquire
Reed Smith LLP
Member

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

James E. Rooks, Jr., Esquire
Center for Constitutional Litigation, P.C.
Member

Andrea D. Rose, Esquire
Crowell & Moring LLP
Participant

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

Ashley Rowe, Esquire
Hunton & Williams LLP
Participant

Elizabeth Sabin
Sabin, Bermant & Gould LLP
Member

Leigh R. Schachter, Esquire
Verizon Wireless
Participant

Gregory P. Schaffer, Esquire
Alltel Corporation
Participant

The Honorable Shira A. Scheindlin
United States District Judge
Southern District of New York
Observer

David Schieferstein, Esquire
Philip Morris USA
Participant

Karl Schieneman, Esquire
Special Counsel
Member

Eric J. Schwarz
Ernst & Young LLP
Participant

Steven Shankroff
Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates
Member

Kenneth Shear, Esquire
SPI Litigation Direct
Participant

James D. Shook
Special Counsel, Inc.
Member

Sonya L. Sigler
Cataphora
Participant

Robert R. Simpson, Esquire
Shipman & Goodwin, LLP
Participant

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

James A. Snyder
BKD, LLP
Member

Kirke Snyder
LECG, LLC
Member

Lisa J. Sotto, Esquire
Hunton & Williams LLP
Member

Ariana J. Tadler, Esquire
Milberg Weiss Bershad & Schulman LLP
Steering Committee Member

Judy Van Dusen
VanKorn Group, Limited
Participant

Robert J. Van Hooser
Deloitte
Member

Lori Ann Wagner, Esquire
Faegre & Benson LLP
Steering Committee Member

Skip Walter
Attenex Corporation
Member

Emroy Watson
Yamaha Motor Corporation
Member

Pola R. Wax
Covington & Burling
Member

Daniel Wentworth
Fidelity Investments
Member

Brian S. Westenberg, Esquire
Miller, Canfield, Paddock & Stone, PLC
Participant

Karl Wiersholm
Messagegate, Inc.
Member

Robert Wiggins, Esquire
Morgan Lewis & Bockius LLP
Member

Robert F. Williams
Cohasset Associates, Inc.
Participant

David Wilson
Ernst & Young LLP
Participant

Scott L. Winkelman, Esquire
Crowell & Moring LLP
Member

Thomas P. Wisinski, Esquire
Haynes & Boone LLP
Member

Kenneth J. Withers, J.D.
Senior Education Attorney
Federal Judicial Center
Observer

Edward C. Wolfe, Esquire
General Motors Corp.
Participant

Gregory B. Wood, Esquire
Fulbright & Jaworski LLP
Participant

Todd I. Woods, Esquire
Lowe's Companies, Inc.
Participant

Susan B. Wortzman, Esquire
Lerners LLP
Participant

Christopher Yowell
Celerity Consulting Group, Inc.
Member

Patrick E. Zeller, Esquire
Seyfarth Shaw LLP
Member

Appendix H: Background on The Sedona Conference® & its Working Group Series

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

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

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

Funding for The Sedona Conference® comes from individuals, law firms and corporations, in the form of donations, sponsorships and registration fees. Funding for the 2005-06 Working Group Addressing Electronic Document Retention and Production came from individual Working Group membership fees, as well as sponsorships provided by *Electronic Evidence Discovery, Inc., Jones Day, Mayer Brown Rowe & Maw LLP (Founding Sponsors), and ARMA International, Bank of America, Carrington Coleman Sloman & Blumenthal, EMC Corporation, Ernst & Young, FTI Consulting, Navigant Consulting, Inc., PricewaterhouseCoopers,* and *Sullivan & Cromwell* (Supporting Sponsors).

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

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

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

wgs

wgs SM

CIVIL DISCOVERY STANDARDS*

AUGUST 2004

*The Standards, which appear in bold face type, were adopted as ABA policy in August 1999 and revised in 2004.

STANDARD

VIII. TECHNOLOGY

1620427.1

VIII. TECHNOLOGY

29. Electronic Information.

a. Identifying Electronic Information. In identifying electronic data that parties may be called upon, in appropriate circumstances, to preserve or produce, counsel, parties and courts should consider:

i. The following types of data:

A. Email (including attachments);

B. Word processing documents;

C. Spreadsheets;

D. Presentation documents;

E. Graphics;

F. Animations;

G. Images;

H. Audio, video and audiovisual recordings; and

I. Voicemail.

ii. The following platforms in the possession of the party or a third person under the control of the party (such as an employee or outside vendor under contract):

A. Databases;

B. Networks;

C. Computer systems, including legacy systems (hardware and software);

D. Servers;

E. Archives;

F. Back up or disaster recovery systems;

G. Tapes, discs, drives, cartridges and other storage media;

H. Laptops;

I. Personal computers;

J. Internet data;

K. Personal digital assistants;

L. Handheld wireless devices;

M. Mobile telephones;

N. Paging devices; and

O. Audio systems, including voicemail.

iii. Whether potentially producible electronic data may include data that have been deleted but can be restored.

b. Discovery of Electronic Information.

i. Document requests should clearly state whether electronic data is sought. In the absence of such clarity, a request for "documents" should ordinarily be construed as also asking for information contained or stored in an electronic medium or format.

ii. A party should specify whether electronic information should be produced in hard copy, in electronic form or, in an appropriate case, in both forms. A party requesting information in electronic form should also consider:

A. Specifying the format in which it prefers to receive the data, such as:

I. Its native (original) format, or

II. A searchable format.

B. Asking for the production of metadata associated with the responsive data — i.e., ancillary electronic information that relates to responsive electronic data, such as information that would indicate whether and when the responsive electronic data was created, edited, sent, received and/or opened.

C. Requesting the software necessary to retrieve, read or interpret electronic information.

D. Inquiring as to how the data are organized and where they are stored.

iii A party who produces information in electronic form ordinarily need not also produce hard copy to the extent that the information in both forms is identical or the differences between the two are not material.

iv. In resolving a motion seeking to compel or protect against the production of electronic information or related software, or to allocate the costs of such discovery, the court should consider such factors as:

A. The burden and expense of the discovery, considering among other factors the total cost of production in absolute terms and as compared to the amount in controversy;

B. The need for the discovery, including the benefit to the requesting party and the availability of the information from other sources;

C. The complexity of the case and the importance of the issues;

D. The need to protect the attorney-client privilege or attorney work product, including the burden and expense of a privilege review by the producing party and the risk of inadvertent disclosure of privileged or protected information despite reasonable diligence on the part of the producing party;

E. The need to protect trade secrets, and proprietary or confidential information;

F. Whether the information or the software needed to access it is proprietary or constitutes confidential business information;

G. The breadth of the discovery request;

H. Whether efforts have been made to confine initial production to tranches or subsets of potentially responsive data;

I. The extent to which production would disrupt the normal operations and processing routines of the responding party;

J. Whether the requesting party has offered to pay some or all of the discovery expenses;

K The relative ability of each party to control costs and its incentive to do so;

L. The resources of each party as compared to the total cost of production;

M. Whether responding to the request would impose the burden or expense of acquiring or creating software to retrieve potentially responsive electronic data or otherwise require the responding party to render inaccessible electronic information accessible, where the responding party

would not do so in the ordinary course of its day-to-day use of the information;

N. Whether responding to the request would impose the burden or expense of converting electronic information into hard copies, or converting hard copies into electronic format;

O. Whether the responding party stores electronic information in a manner that is designed to make discovery impracticable or needlessly costly or burdensome in pending or future litigation, and not justified by any legitimate personal, business, or other non-litigation related reason; and

P. Whether the responding party has deleted, discarded or erased electronic information after litigation was commenced or after the responding party was aware that litigation was probable and, if so, the responding party's state of mind in doing so.

v. In complex cases and/or cases involving large volumes of electronic information, the court may want to consider using an expert to aid or advise the court on technology issues

vi. The parties are encouraged to stipulate as to the authenticity and identifying characteristics (date, author, etc.) of electronic information that is not self-authenticating on its face.

2004 Comment

Subdivision(a)

Subdivision (a)(i). Standard 29(a)(i) is principally designed to provide a checklist to assist counsel in identifying types of electronic data as to which the duty to preserve may apply, once that duty has been triggered under applicable law. *See, e.g., Super Film of Am., Inc. v. UCB Films, Inc.*, 219 F.R.D. 649, 657 (D. Kan. 2004) (for purposes of Federal Rule of Civil Procedure 26, "[c]omputerized data and other electronically-recorded information includes, but is not limited to: voice mail messages and files, back-up voice mail files, e-mail messages and files, backup e-mail files, deleted e-mails, data files, program files, backup and archival tapes, temporary files, system history files, web site information stored in textual, graphical or audio format, web site log files, cache files, cookies, and other electronically-recorded information") (citation and quotations omitted).

This Standard is not intended to suggest that electronic discovery is appropriate in all cases. There may be many cases in which electronic discovery is not warranted, in light of the amount in controversy or any number of other reasons.

The deletion of the former first sentence of subdivision (a)(i) is intended to clarify that the Standards do not create or codify law but rather defer to governing substantive law. The purpose of the list provided in subdivision (a)(i) is to assist counsel in protecting client interests under whatever strictures may be imposed by governing law. It is not to suggest that every item in the list is applicable in every case or that counsel has any duty to instruct a client to preserve any, much less every, item on the list. All duties are dictated by governing state or federal law and not by this or any other of these Standards.

Subdivision (a)(ii). Just as subdivision (a)(i) provides a checklist of the types of electronic data that counsel should bear in mind, Standard 29(a)(ii) provides a checklist of platforms and places where such data may be found. As with subdivision (a)(i), subdivision (a)(ii) does not create a preservation duty. Rather, it is another reference tool intended to be consulted once the duty to preserve electronic data has accrued under local law.

Subdivision (a)(iii). Standard 29(a)(iii) is simply a reminder that, as is well established in the case law, when a preservation duty has been triggered, it may be found to apply to "deleted" information remaining on the hard drive of the computer. *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 313 n.19 (S.D.N.Y. 2003) ("The term 'deleted' is sticky in the context of electronic data. 'Deleting' a file does not actually erase that data from the computer's storage devices. Rather, it simply finds the data's entry in the disk directory and changes it to a 'not used' status -- thus permitting the computer to write over the 'deleted' data. Until the computer writes over the 'deleted' data, however, it may be recovered by searching the disk itself rather than the disk's directory. Accordingly, many files are recoverable long after they have been deleted -- even if neither the

computer user nor the computer itself is aware of their existence. Such data is referred to as 'residual data.'")(internal quotations and citation omitted).

Former Subdivision (a)(ii). Former subdivision (a)(ii) has been moved to subdivision (b), where it conceptually belongs, as new subdivision (b)(i), with minor modification.

Former Subdivision (a)(iii). Former subdivision (a)(iii) has been deleted. As drafted, it appeared to create or codify a proposition of law, which is not the proper function of a Standard. Moreover, the law is evolving swiftly in the area of electronic discovery and, as stated, the deleted language is not necessarily good law. *See, e.g., Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 324 (S.D.N.Y. 2003) ("because the cost-shifting analysis is so fact-intensive, it is necessary to determine what data may be found on the inaccessible media. Requiring the responding party to restore and produce responsive documents from a small sample of the requested backup tapes is a sensible approach in most cases").

Subdivision(b)

Subdivision (b)(i). The second sentence of subdivision (b)(i) is the former subdivision (a)(ii), with the addition of a connecting dependent clause and the insertion of the modifier "ordinarily," the latter in recognition of the fact that there may be unusual circumstances in which the stated presumption is obviously inapt. The new first sentence is added as a "best practices" reminder to counsel.

Subdivision (b)(ii). Subdivision (b)(ii) restates and expands the former subdivision (b)(i). The substantive additions are to remind counsel, first, that they have the option of specifying the format in which they wish to receive the desired data and, second, that they may want to inquire as to how the data were organized and where they were stored, since this information may be lost in electronic production.

Subdivision (b)(iii). Subdivision (b)(iii) combines the former subdivisions (b)(ii) and (b)(iv) in recognition of the fact that the factors applied by the courts in resolving motions to compel (or resist production) and motions to allocate costs are largely the same. Additionally, subdivision (b)(iii) expands the former subdivisions (b)(ii) and (b)(iv) to capture additional factors that experience and the developing case law have identified as pertinent to the court's decision. Among the authorities relied on in the recitation of factors in this subdivision are: Federal Judicial Center, Manual for Complex Litigation § 11.446 (4th ed. 2004); 7 Moore's Federal Practice §§ 37a.30-33 (3d ed. 2004); *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003); *Computer Associates International, Inc. v. Quest Software, Inc.*, No. 02-C-4721, 2003 WL 21277129 (N.D. Ill. June 3, 2003); *Medtronic Sofamor Danek, Inc. v. Michelson*, No. 01-2373-M1V, 2003 WL 21468573 (W.D. Tenn. May 13, 2003); *Dodge, Warren, & Peters Ins. Servs. v. Riley*, 130 Cal. Rptr. 2d 385 (Cal. App. 2003); *Byers v. Illinois State Police*, 2002 WL 1264004 (N.D. Ill. June 3, 2002); *Southern Diagnostic Assocs. v. Bencosme*, 833 So.2d 801 (Fla. App. 2002); *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, 2002 WL 246439 (E.D. La. Feb. 19, 2002); *Rowe Entertainment, Inc. v. William Morris Agency*, 205 F.R.D. 421 (S.D.N.Y. Jan 16, 2002); *In re CI Host, Inc.*, 92 S.W. 3d 514 (Tex. 2002); *In re Bristol-Meyers Squibb Secs. Litig.*, 205 F.R.D. 437 (D.N.J. 2002); *McPeek v. Ashcroft*, 202 F.R.D. 31 (D.D.C. Aug. 1, 2001); McCurdy *Group, LLC v. American Biomedical Group, Inc.*, Nos. 00-6183, 00-6332, 2001 WL 536974 (10th Cir. May 21, 2001).

Subdivision (b)(iv). Subdivision (b)(iv) is the former subdivision (b)(v) unchanged.

Former Subdivision (b)(ii). Former subdivision (b)(ii), together with former subdivision (b)(iv), is contained within new subdivision (b)(iii).

Former Subdivision (b)(iii). Former subdivision (b)(iii) has been deleted. As drafted, it appeared to create or codify a proposition of law, which is not the proper function of a Standard. Moreover, the law is evolving swiftly in the area of electronic discovery and, as stated, the deleted language is not necessarily good law. *See, e.g., Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 324 (S.D.N.Y. 2003).

Former Subdivision (b)(iv). Former subdivision (b)(iv), together with former subdivision (b)(ii), is contained within new subdivision (b)(iii).

30. **Using Technology to Facilitate Discovery.**

    a. **In appropriate cases, the parties may agree or the court may direct that some or all discovery materials that have not been stored in electronic form should nonetheless be produced, at least in the first instance, in an electronic format and how the expenses of doing so will be allocated among the parties.**

    b. **A party serving written discovery requests or responses should provide the other party or parties with an electronic version of the requests or responses unless the parties have previously agreed that no electronic version is required.**

2004 Comment

Subdivision (a). This change is not substantive but merely clarifying. If the data sought in discovery already exist in electronic form, there is no need for a court order requiring their production in that format. This subdivision is directed at the production in electronic format of data not currently stored electronically. The amendment makes that clear.

Subdivision (b). Subdivision (b) has been amended to interpose a presumption where previously a request was suggested. As amended, this subdivision affirmatively recommends that counsel provide adversaries with discovery requests or responses in electronic format unless the parties have previously agreed to the contrary. Because the Standard is purely precatory, it imposes no duty. Rather, it recommends a practice for counsel to consider.

31. **Discovery Conferences.**

    a. **At the initial discovery conference, the parties should confer about any electronic discovery that they anticipate requesting from one another, including:**

        i. **The subject matter of such discovery.**

        ii. **The time period with respect to which such discovery may be sought.**

        iii. **Identification or description of the party-affiliated persons, entities or groups from whom such discovery may be sought.**

        iv. **Identification or description of those persons currently or formerly affiliated with the prospective responding party who are knowledgeable of the information systems, technology and software necessary to access potentially responsive data.**

        v. **The potentially responsive data that exist, including the platforms on which, and places where, such data may be found as set forth in Standard 29 (a).**

        vi. **The accessibility of the potentially responsive data, including discussion of software, hardware or other specialized equipment that may be necessary to obtain access.**

        vii. **Whether potentially responsive data exist in searchable form.**

        viii. **Whether potentially responsive electronic data will be requested and produced:**

            A. **In electronic form or in hard copy, and**

            B.**If in electronic form, the format in which the data exist or will be pro**

        ix. **Data retention policies applicable to potentially responsive data.**

x. Preservation of potentially responsive data, specifically addressing (A) preservation of data generated subsequent to the filing of the claim, (B) data otherwise customarily subject to destruction in ordinary course, and (C) metadata reflecting the creation, editing, transmittal, receipt or opening of responsive data.

xi. The use of key terms or other selection criteria to search potentially responsive data for discoverable information.

xii. The identity of unaffiliated information technology consultants whom the litigants agree are capable of independently extracting, searching or otherwise exploiting potentially responsive data.

xiii. Stipulating to the entry of a court order providing that production to other parties, or review by a mutually-agreed independent information technology consultant, of attorney-client privileged or attorney work-product protected electronic data will not effect a waiver of privilege or work product protection.

xiv. The appropriateness of an inspection of computer systems, software, or data to facilitate or focus the discovery of electronic data.

xv. The allocation of costs.

b. At any discovery conference that concerns particular requests for electronic discovery, in addition to conferring about the topics set forth in subsection (a), the parties should consider, where appropriate, stipulating to the entry of a court order providing for:

i. The initial production of tranches or subsets of potentially responsive data to allow the parties to evaluate the likely benefit of production of additional data, without prejudice to the requesting party's right to insist later on more complete production.

ii. The use of specified key terms or other selection criteria to search some or all of the potentially responsive data for discoverable information, in lieu of production.

iii. The appointment of a mutually-agreed, independent information technology consultant pursuant to Standard 32(a) to:

A. Extract defined categories of potentially responsive data from specified sources, or

B. Search or otherwise exploit potentially responsive data in accordance with specific, mutually-agreed parameters.

2004 Comment

The Federal Rules of Civil Procedure require a discovery conference at the outset of every case and prior to the filing of any discovery motion. Practices vary district by district. State court practice varies state by state, but a conference early in the case is sensible in connection with electronic discovery, regardless of whether it is compelled. Standard 31 focuses on effective use of discovery conferences to address electronic discovery issues.

Subdivision (a). Subdivision (a) focuses on the initial discovery conference. It specifies several categories of electronic discovery related matters that the parties should confer about at an initial discovery conference. It is intended to assist counsel and the court by providing a detailed array of potentially relevant issues to address. These include:

- Subject matter
- Relevant time period
- Identification of the party-affiliated persons or entities from whom electronic discovery may be sought
- Identification of those persons (including former employees) who are knowledgeable of the information systems, technology and software necessary to access potentially responsive data

- The universe of potentially responsive data that exist, including the platforms on which, and places where, such data may be found (including databases, networks, systems, servers, archives, back up or disaster recovery systems, tapes, discs, drives, cartridges and other storage media, laptops, PCs, Internet data, and PDAs)
- Accessibility issues, such as the software that may be necessary to access data
- Whether potentially responsive data exist in searchable form
- Whether potentially responsive electronic data will be requested and produced in electronic form or in hard copy
- Data retention policies
- Preservation issues, including preservation of data generated subsequent to the filing of the claim
- Possible use of key terms or other selection criteria to scour massive amounts of data for relevant information

Anticipating the privilege-related issues addressed in Standard 32, subdivision (a)(xii) suggests that the parties discuss whether they can agree on the names of unaffiliated information-technology consultants who would be capable of serving them jointly, either in a privately-retained or court-appointed capacity. In the same vein, subdivision (a)(xiii) proposes that the parties consider whether it would be desirable for them to stipulate to entry of a court order along the lines discussed in Standard 32(b) or (c).

Subdivision (b). Subdivision (b) focuses on discovery conferences relating to outstanding discovery requests (in common parlance, the "meet-and-confer"). It recognizes that there are additional issues for the parties to consider once discovery demands have been served and specific issues are on the table. Subdivision (b) anticipates a number of the privilege-related initiatives contained in Standard 32, recommending that the parties consider stipulating to a court order providing for:

- Initial production, on a without-prejudice basis, of subsets of electronic data to allow the parties to evaluate the likely benefit of production of additional data;
- The use of search terms or other selection criteria in lieu of production; or
- The appointment of an independent consultant pursuant to Standard 32

1620427.1

32. Attorney-Client Privilege and Attorney Work Product.

To ameliorate attorney-client privilege and work product concerns attendant to the production of electronic data, the parties should consider, where appropriate, stipulating to the entry of a court order:

a. Appointing a mutually-agreed, independent information technology consultant as a special master, referee, or other officer or agent of the court such that extraction and review of privileged or otherwise protected electronic data will not effect a waiver of privilege or other legal protection attaching to the data.

b. Providing that production to other parties of attorney-client privileged or attorney work-product protected electronic data will not effect a waiver of privilege or work product protection attaching to the data. In stipulating to the entry of such an order, the parties should consider the potential impact that production of privileged or protected data may have on the producing party's ability to maintain privilege or work-product protection vis-à-vis third parties not subject to the order.

c. Providing that extraction and review by a mutually-agreed independent information technology consultant of attorney-client privileged or attorney work-product protected electronic data will not effect a waiver of privilege or work product protection attaching to the data.

d. Setting forth a procedure for the review of the potentially responsive data extracted under subdivision (a), (b), or (c). The order should specify that adherence to the procedure precludes any waiver of privilege or work product protection attaching to the data. The order may contemplate, at the producing party's option:

i. Initial review by the producing party for attorney-client privilege or attorney work product protection, with production of the unprivileged and unprotected data to follow, accompanied with a privilege log, or

ii. Initial review by the requesting party, followed by:

A. Production to the producing party of all data deemed relevant by the requesting party, followed by

B. A review by the producing party for attorney-client privilege or attorney work product protection. Before agreeing to this procedure, the producing party should consider the potential impact that it may have on the producing party's ability to maintain privilege or work-product protection attaching to any such data if subsequently demanded by non-parties.

The court's order should contemplate resort to the court for resolution of disputes concerning the privileged or protected nature of particular electronic data.

e. Prior to receiving any data, any mutually-agreed independent information technology consultant should be required to provide the court and the parties with an affidavit confirming that the consultant will keep no copy of any data provided to it and will not disclose any data provided other than pursuant to the court's order or parties' agreement. At the conclusion of its engagement, the consultant should be required to confirm under oath that it has acted, and will continue to act, in accordance with its initial affidavit.

f. If the initial review is conducted by the requesting party in accordance with subsection (d)(ii), the requesting party should provide the court and the producing party an affidavit stating that the requesting party will keep no copy of data deemed by the producing party to be privileged or work product, subject to final resolution of any dispute by the court, and will not use or reveal the substance of any such data unless permitted to do so by the court.

1620427.1

2004 Comment

Standard 32 deals with privilege and work product (collectively, "privilege") concerns. It applies in the common situation in which electronic data must be extracted for production by an information technology (IT) expert not employed by the producing party. This scenario by definition raises a risk of waiver because privileged documents are being exposed to persons outside the privilege. Standard 32 sets forth three methods to ameliorate the risk of waiver. Each would be implemented by entry of a stipulated court order.

Subdivision (a). Subdivision (a) suggests that the parties consider having the court appoint a mutually-agreed IT consultant as a special master, referee, or other officer of the court, so that the consultant's extraction and review of privileged electronic data will not effect a waiver. This approach would allow the third party consultant to pull and have access to privileged material (which may be included in any mass extraction of data) without risk that the holder of the privilege will have effected a waiver by permitting the third party to review them. Following extraction, the parties are then free to specify whatever protocol they prefer with respect to review of the data. This is addressed in subdivision (d).

Subdivision (b). Subdivision (b) addresses what is sometimes known as the "quick peek" approach to electronic discovery. Under the quick-peek scenario envisioned by subdivisions (b) and (d)(ii), the requesting party may have sufficient resources to perform or pay for the extraction, and the producing party may be inclined to allow its opponent to incur all expenses associated with doing so. At the same time, the producing party has no interest in waiving privilege. The parties therefore agree that the data will be turned over to the requesting party without review by the producing party; the requesting party will identify which documents it is interested in, and the producing party will then conduct a privilege review. Subdivision (b) captures the court order necessary to permit this procedure to proceed.

Under subdivision (b), the parties stipulate to an order providing that production of privileged electronic data will not effect a waiver. Note that this is different from the customary agreed order, which provides that inadvertent production will not effect a waiver, because parties using the subdivision (b) approach may know or be fairly certain that privileged material is contained in the mass of data to be extracted. Like that order, however, there is some question as to the effectiveness of such an order *vis-à-vis* a third party who subsequently seeks the disclosed data. Accordingly, there is an appropriate caution in the text of this subdivision and in subdivision (d)(ii).

Subdivision (c). Subdivision (c) is similar to subdivision (a) in that it envisions the use of an agreed third-party consultant. Under subdivision (c), unlike subdivision (a), that consultant is not appointed as a special master or other court officer. The court, for example, may not be inclined to appoint the consultant as a master or the parties may prefer to control the consultant directly. Subdivision (c) is also similar to subdivision (b) in that it envisions the entry of an order providing that review of intentionally-produced privileged data will not effect a waiver. But the reviewing party under subdivision (c) is an agreed-on consultant, not the opposition. As under both subdivisions (a) and (b), under subdivision (c) the parties are free to specify whatever protocol they prefer with respect to review of the data, following extraction. This is addressed in subdivision (d).

As observed in the comment to subdivision (b), *supra*, in current practice, there is no assurance that a stipulated order providing that inadvertent production does not effect a waiver will be effective against a claim of waiver asserted by a third party. Precisely the same risk is posed by the order envisaged by subdivision (c). Accordingly, it is imperative that litigants following either of these routes also have in place a confidentiality order as a second line of defense against inquisitive third parties. It is equally important that the litigants develop a protocol for, or otherwise instruct, the consultant to minimize the likelihood that the consultant will actually review (as opposed to extract) privileged material.

Subdivision (d). Subdivision (d) sets forth a pair of alternative procedures for the parties to consider with respect to the review of the data once the data have been extracted. Subdivision (d)(i) states that traditional approach, in which the extracted data are furnished to the producing party, who then conducts a review for responsiveness and privilege, and makes production of the data together with a privilege log.

Subdivision (d)(ii) identifies an unconventional approach that some parties prefer for financial reasons, as where there is an enormous amount of electronic data, little of it is likely to be either responsive or privileged, and little of that will fall in both categories. Under the (d)(ii) approach, the requesting party first reviews the data for responsiveness and provides to the producing party all data in which it is interested. The producing party then determines if any of the data in question are privileged. If so, the requesting party may not maintain copies of the

privileged material unless and until a court sustains its objections to the claim of privilege. This procedure raises the risk of waiver of privilege identified in the comment to subdivision (b). Accordingly, the text of subdivision (d)(ii)(B) contains substantially the same caution as that set forth in subdivision (b).

Subdivision (e). Subdivision (e) suggests a reasonable precaution — that any IT consultant employed by the parties be required to execute an affidavit confirming that it will keep no copy of any data and will not disclose any data provided other than pursuant to the court's order or parties' agreement.

Subdivision (f). Subdivision (f) provides that, before receiving the data pursuant to subdivision (d)(ii), the requesting party is to execute an affidavit stating that it will keep no copy of data deemed by the producing party to be privileged, subject to final resolution of any dispute by the court. This precaution is appropriate in light of the trust that the producing party reposes in the requesting party under the quick-peek approach captured in subdivisions (b) and (d)(ii).

33. Technological Advances. To the extent that information may be contained or stored in a data compilation in a form other than electronic or paper, it is intended that Standards 29-32 may be consulted with respect to discovery of such information, with appropriate modifications for the difference in storage medium.

2004 Comment

Standard 33 recognizes the impracticability of keeping pace with technological change. New, non-electronic media may emerge for the creation or retention of electronic data. This Standard suggests that Standards 29-32 be consulted with respect to discovery of such data, subject to common sense modifications.

11 MITTLR 71
11 Mich. Telecomm. & Tech. L. Rev. 71
(Cite as: 11 Mich. Telecomm. & Tech. L. Rev. 71)

Michigan Telecommunications and Technology Law Review
Fall 2004

Article

***71** ELECTRONIC DISCOVERY SANCTIONS IN THE TWENTY-FIRST CENTURY

Shira A. Scheindlin [FNa1]
Kanchana Wangkeo [FNaa1]

Cite as: Shira A. Scheindlin and Kanchana Wangkeo, Electronic Discovery Sanctions in the Twenty-First Century,11 Mich. Telecomm. Tech. L. Rev. 71 (2004),available at http://www.mttlr.org/voleleven/scheindlin.pdf

I. Introduction

Liberal discovery is a hallmark of our civil justice system because parties need information to prosecute or defend their cases. Relevant information may be conveyed to the adversary in a myriad of ways, including pretrial disclosures, responses to interrogatories, and an exchange of documents. In today's paperless world, discovery has focused less on hard copy documents and more on electronically-stored information. Requests for electronic information have become so commonplace that one judge has remarked, "[I]t is black letter law that computerized data is discoverable if relevant." [FN1]

A problem with discovering electronic data, however, is that it is much more susceptible to unintentional destruction than

11 MITTLR 71
11 Mich. Telecomm. & Tech. L. Rev. 71
(Cite as: 11 Mich. Telecomm. & Tech. L. Rev. 71)

hard copy documents. Electronic data is often recycled or overwritten as part of normal business practices because a business cannot or need not retain large volumes of outdated information. When litigation ensues, companies need to take affirmative steps to prevent the destruction of certain relevant electronic documents, such as e-mails, computer records, and possibly back-up tapes. Not surprisingly, spoliation has become a significant e-discovery problem, and businesses have expressed the need for ***72** a "safe harbor" to protect themselves from sanctions for the inadvertent loss of electronic documents. [FN2]

Parties may be sanctioned for spoliation under Federal Rule of Civil Procedure 37, a state-law equivalent of Rule 37, or a court's inherent power. [FN3] Rule 37 does not specifically authorize a court to impose sanctions for the spoliation of evidence. However, courts frequently rely on subsections (b) and (c) of Rule 37 when imposing such sanctions because a party has destroyed documents in violation of a court order or the destruction of documents has rendered a party unable to comply with its disclosure obligations under the Rules. Subsection (b) provides: "[I]f a party fails to obey an order entered under Rule 26(f), the court in which the action is pending may make such orders in regard to the failure as are just . . . ." Subsection (c) permits a court to "impose other appropriate sanctions" if a party "without substantial justification fails to disclose information required by Rule 26(a) or 26(e)(1), or to amend a prior response to discovery as required by Rule 26(e)(2)."

At the federal level, the Civil Rules Advisory Committee has responded to the "unique and necessary feature of computer systems--the automatic recycling, overwriting, and alteration of electronically stored information" [FN4]--with a proposed amendment to Rule 37. The proposed Rule 37(f) would shield litigants from sanctions for the destruction of electronic data if the party "took reasonable steps to preserve the information after it knew or should have known the information was discoverable in the action" and "the failure resulted from the loss of the information because of the routine operation of the party's electronic information system." [FN5] The safe harbor provision would not apply if "a party violated an order in the action requiring it to preserve electronically stored information." [FN6]

This proposed rule is controversial for several reasons. Businesses have complained that reform is needed because requiring them to store and retrieve electronic information is expensive and burdensome--much more so than with paper documents. Although the proposal acknowledges the need to recycle electronic data regularly, it does not provide the broad protection sought by the business community to forbid sanctions in the absence of willful or reckless conduct. In addition, some view the proposed rule as insufficient because it may not adequately address the prejudice caused to the party that can no longer obtain information that has been destroyed. To the extent the rule is perceived ***73** as a blank check to destroy electronic information with impunity, [FN7] however, that criticism is misplaced. Proposed Rule 37(f) provides that a company cannot be punished merely for the routine recycling of information. If the company knows or should know that electronic information is discoverable in the action or if the court issues a preservation order, the company must take reasonable steps to preserve the information.

The shape and form of a safe harbor provision--or even the need for one--can only be understood by analyzing how courts have been addressing this problem in the absence of such a rule. Have courts sanctioned parties for conduct that is merely negligent, as opposed to willful or reckless? Have they insisted on a showing of prejudice before they will sanction parties for spoliation? Have parties generally deserved the sanctions they received? In an attempt to provide guidance to the legal community, we have surveyed recent written opinions on this topic to determine how courts have defined sanctionable conduct and what sanction has been imposed for such conduct.

Our sample consisted of all the written opinions in the sanctions arena since January 1, 2000: [FN8] 45 federal cases, and 21 state cases. We included state cases in the sample because spoliation issues are not confined to federal court. We limited the sample to the twenty-first century because we believed recent cases would be the most indicative of whether courts had appropriately adapted to e-discovery issues caused by technological advancements. Although we are pleased to report that courts seem to be "getting it right," our analysis is necessarily limited by our small sample and cannot be applied to sanctions cases generally. [FN9] ***74** Because we could only locate and analyze written opinions, the sample is undoubtedly skewed in favor of cases granting sanctions. Many sanctions decisions are issued from the bench, and courts are less likely to issue written opinions when they are denying sanctions than when they are granting them.

With those caveats in mind, we now turn to the substance of the survey. Part II of this Article summarizes the data gleaned from the cases, while Part III interprets the data. Part III also highlights representative cases in which sanctions were granted or denied and the reasoning behind those decisions. The Article concludes with a discussion of how our survey can inform the current debate on e-discovery reform.

11 MITTLR 71
11 Mich. Telecomm. & Tech. L. Rev. 71
(Cite as: 11 Mich. Telecomm. & Tech. L. Rev. 71)

II. Summary of Data

In written opinions, requests for sanctions arose most often in tort (24%) [FN10] and intellectual property cases (20%), [FN11] followed by contract ***75** (18%), [FN12] and employment (15%) [FN13] cases. The remaining 23% involved various subject matters. [FN14]

Courts granted sanctions 65% of the time, [FN15] with defendants being sanctioned four times (81%) [FN16] as often as plaintiffs ***76** (19%). [FN17] The sanctioned behavior most often involved the non-production, i.e., destruction of electronic documents (84%), [FN18] rather than a delay in production (16%). [FN19] When parties were sanctioned for delay, the late production was sometimes coupled with some form of deception or misrepresentation to the court, such as the fabrication of evidence or falsely claiming that documents did not exist (43%). [FN20]

Often, the sanctioned party had violated a court order (53%), [FN21] though not necessarily a specific order to preserve documents (16%). [FN22] Spoliation also occurred where there were general discovery (30%) [FN23] or injunctive orders in place (7%). [FN24] When courts imposed sanctions, they ***77** referred to the willfulness or bad faith of the violator (49%), [FN25] prejudice to the party requesting production (35%), [FN26] and/or the gross negligence or recklessness of the spoliating party (9%), [FN27] as the reason(s) for imposing the sanction(s).

Attorney's fees and costs were the most frequently granted sanction (60%). [FN28] Courts granted evidentiary sanctions, such as preclusion (30%), [FN29] adverse inference instructions (23%) [FN30] and dismissal or default ***78** judgments (23%) [FN31] with less frequency. The types of sanctions ordered were not mutually exclusive, with courts imposing more than one sanction 28% of the time. [FN32] Courts based their authority to impose sanctions on Rule 37 (57% of federal cases), [FN33] state law (40% of state cases), [FN34] and their inherent power (28%). [FN35] In 37% of the cases where sanctions were issued, the court cited no authority whatsoever. [FN36]

***79** In 35% of all the cases examined, [FN37] sanctions were not imposed even though a party had destroyed electronic data (87%) [FN38] or had violated a court order (39%). [FN39] In some instances, the court declined to impose a sanction because it was too early to determine the extent of the harm involved. [FN40] Of these cases where sanctions were not imposed, 17% involved appellate courts reversing judgments because the district courts had failed to properly consider the need for e-discovery sanctions. [FN41] When sanctions were denied, the usual reasons were lack of willfulness ***80** or bad faith (35%), [FN42] and/or lack of prejudice (30%). [FN43] A small percentage of sanctions motions were held to be premature (17%) [FN44] or denied for a variety of other reasons (30%). [FN45]

In short, the results of our survey reveal that the profile of a typical sanctioned party is a defendant that destroys electronic information in violation of a court order, in a manner that is willful or in bad faith, or causes prejudice to the opposing party.

III. Interpretation of Data

A. Prejudice

Appellate courts have made clear that a finding of bad faith is not required to impose discovery sanctions. [FN46] Indeed, bad faith was not present ***81** in most of the cases in our sample, and courts often imposed discovery sanctions where there was a lesser degree of culpability by the offending party, or cognizable prejudice to the injured party.

In cases where a party has been prejudiced by the spoliation of electronic documents, courts have imposed sanctions aimed at restoring the prejudiced party to the position she would have been in had the documents not been destroyed. Courts often sought to remedy the prejudice through an evidentiary sanction or an adverse inference instruction. [FN47]

***82** For instance, in Thompson v. U.S. Department of Housing and Urban Development, Magistrate Judge Paul Grimm precluded certain defendants from using 80,000 e-mails for trial purposes because defendants produced them long after the discovery cutoff deadline, contradicting their prior representations that the e-mails did not exist or had already been produced. [FN48] The magistrate judge concluded that defendants had violated earlier orders of the court by failing to produce electronic records, and that Rule 37(b) sanctions were justified because defendants' non-compliance was not substantially justified and was also prejudicial to the plaintiffs. [FN49] In considering the remedy, the judge reasoned that "there was no effective way to cure the surprise" short of postponing the trial date and reopening discovery, given the volume

11 MITTLR 71
11 Mich. Telecomm. & Tech. L. Rev. 71
(Cite as: 11 Mich. Telecomm. & Tech. L. Rev. 71)

of e-mails, the fact that discovery had been closed for months (thereby preventing plaintiffs from using the e-mails during depositions), and trial was set to begin in approximately ninety days. [FN50] The judge noted that the case had been aggressively litigated for nine years, and that the court had given unambiguous signals to counsel that the trial date would not be postponed. [FN51]

Ultimately, Magistrate Judge Grimm modified his order precluding three witnesses from testifying because that sanction would have deprived defendants of the ability to prove their defenses. Instead, the magistrate judge precluded defendants from introducing any of the 80,000 e-mails into evidence; forbid defense counsel from using them to prepare or refresh the recollection of trial witnesses; and permitted plaintiffs to use them in their direct and cross-examinations. [FN52] Plaintiffs were also permitted to request further sanctions if they incurred additional expenses and attorney's fees in connection with the e-mails or if the evidence revealed additional information regarding the non-production of e-mail records. [FN53] An adverse inference instruction was not appropriate because it was a bench trial, and the judge would be able to draw reasonable inferences from the failure to preserve and produce documents as ordered. [FN54] By these means, the court felt it was able to remedy plaintiffs' disadvantage.

***83** Where there is no effective way to cure the prejudice, however, a court may dismiss the claims or grant a default judgment in favor of the prejudiced party. For example, in Playball at Hauppauge, Inc. v. Narotzky, the court dismissed plaintiff's breach of fiduciary duty claim because the deletion of computer data by the plaintiff's son left defendant without the ability to defend against plaintiff's allegations of mismanagement and waste. [FN55]

Conversely, some courts have denied sanctions where the requesting party did not demonstrate that it had been prejudiced by the other party's e-discovery violations. [FN56] In YCA, LLC v. Berry, defendant Berry moved to strike the testimony of YCA's computer expert, and his findings, because YCA had withheld the expert's name from its interrogatory and document production responses and later misled defense counsel into thinking the expert would not be examining Berry's computer. [FN57] Berry's counsel had been informed that YCA's expert would be analyzing the computers of certain persons, but did not specifically name Berry. [FN58] Berry argued that he had been prejudiced because he prepared his summary judgment motion without full knowledge of YCA's case against him. [FN59] In declining to grant the sanction, the court reasoned that YCA's two-week delay in disclosing its use of a computer forensics expert did not create any appreciable prejudice to Berry. [FN60] Furthermore, Berry's belated charge of alleged misrepresentations by YCA deprived YCA of the opportunity to respond. [FN61]

***84** These cases demonstrate that prejudice is a significant factor in assessing whether parties should be sanctioned for e-discovery violations--even where the spoliating party acted willfully or in bad faith. To the party that cannot prosecute or defend its case, it does not matter if the producing party did not intend to delete relevant electronic data; the information is gone, and the party has been hurt by it. When weighing the level of fault against the extent of the harm, courts have exercised their discretion to protect the party seeking discovery when justice so required.

B. Willfulness or Bad Faith

On the other hand, courts have been less concerned with proof of prejudice when faced with willful or bad faith conduct. [FN62] In circumstances ***85** where the conduct is particularly egregious, courts have granted the ultimate sanction of dismissal or default judgment in order to deter obstructionist behavior. [FN63] In those cases, however, the courts have sometimes noted that the party requesting the documents had suffered prejudice as well. [FN64]

Judge Susan Forsling's decision in Mariner Health Care, Inc. v. PricewaterhouseCoopers LLP is instructive of the danger of flouting a court's authority during discovery. [FN65] The judge dismissed Mariner's complaint with prejudice because of its failure to timely produce documents. [FN66] Essentially, Mariner had missed several production deadlines and eventually dumped large volumes of documents, including electronic images, on PricewaterhouseCoopers ("PwC") shortly before the start of depositions, which precluded PwC from taking any depositions. Yet Mariner had produced 22 million pages of documents, and the trial date was two years away. At first glance, Mariner appears to be a case in which the judge imposed a sanction that was disproportionate to the misconduct. Upon closer inspection, however, the case comports with the body of precedent in which sanctions are imposed to deter recalcitrant behavior by litigants.

Mariner was not a simple case of delayed production, but rather a case of systematic discovery abuse. Before being sanctioned, Mariner had violated no less than three separate orders of the court and did so ***86** repeatedly. [FN67] The orders

11 MITTLR 71
11 Mich. Telecomm. & Tech. L. Rev. 71
(Cite as: 11 Mich. Telecomm. & Tech. L. Rev. 71)

contained production deadlines negotiated by the parties and approved by the court, and the judge expressly warned Mariner that it could not simply disregard the orders it found to be unduly burdensome or inconvenient; if it could not comply, it needed to seek relief from the court. [FN68] At the time the judge gave her warning to Mariner, she also reserved ruling on PwC's request for attorney's fees in connection with Mariner's previous discovery violations. [FN69] Judge Forsling informed the parties that she hoped the threat of monetary sanctions "as a 'hammer over Mariner's head' would be more effective than actually awarding fees." [FN70]

Nonetheless, Mariner repeatedly ignored the court's orders and explicit warning "with conscious indifference to the consequences of those violations." [FN71] Mariner consistently produced large volumes of documents late, while insisting that PwC adhere to the discovery schedule, which called for depositions shortly after the documents were delivered. [FN72] Yet Mariner was aware that the discovery schedule was designed to ensure that all parties' interests were protected while the case proceeded in an expeditious manner, i.e., it balanced Mariner's desire for an early trial date with PwC's need to prepare its defense, by having adequate time to review documents in preparation for depositions. [FN73] Although Mariner claimed that the late productions were due to vendor error, it provided no evidence to that effect, and the judge doubted the veracity of its claims given the number of times it had been before the court and kept silent about any alleged problems. [FN74]

Judge Forsling considered awarding PwC's attorney's fees or extending all of the deadlines. However, she concluded that "lesser sanctions would not change Mariner's conduct going forward and would not ensure [the] Court's ability to administer the case justly and efficiently." [FN75] She went on to say:

> There comes a point when the Court, to protect the integrity of its Orders and the purposes of [state law], must take action which sends the message: "Enough is enough." This Court is at ***87** the point in this case. Therefore, no sanction less severe than dismissal of Mariner's complaint with prejudice would be appropriate under these circumstances. [FN76]

The judge also expressly rejected Mariner's argument that prejudice was required for the imposition of sanctions, stating that a requirement of prejudice

> would essentially allow a party that has violated the Court's orders to defeat a motion for sanctions by belatedly complying with the Court's orders and then arguing that its non-compliance has not caused prejudice to the opposing party. In other words, the integrity of the Court's orders and the ability of the Court to control the proceedings would be secondary to the prejudice to the movant, a proposition that this Court is not willing to adopt. [FN77]

Notwithstanding her rejection of a prejudice requirement, the judge did find that PwC had suffered prejudice because until PwC filed its motion for sanctions, Mariner refused to extend the start of depositions, which prejudiced PwC in its preparations. [FN78] Moreover, pushing back the scheduling order deadlines would significantly delay the trial date, allowing witnesses' memories to fade and evidence to become stale. [FN79] Despite finding prejudice, the tenor of the opinion reveals that the court's focus was on the plaintiff's bad faith.

In an ironic twist, PwC is now facing sanctions for its own e-discovery violations. In In re Telxon Securities Litigation, Magistrate Judge Patricia Hemann has recommended that a default judgment be entered against PwC for its failure to preserve documents (including electronic information), incomplete production of relevant information, and the destruction of documents (including electronic information). [FN80] Magistrate Judge Hemann summarized PwC's violations as follows: At the outset of the discovery process, PwC failed to check thoroughly its local servers and its archives for relevant documents, failed to compare the various versions of relevant documents in those databases, failed to produce documents as they were kept in the ordinary course of business, and failed to reproduce thoroughly and accurately all documents and their attachments. [FN81] Prior to the filing of this litigation, PwC had permitted documents to be destroyed even though it had promised to preserve ***88** these documents. [FN82] Despite these failures, PwC repeatedly told the court and the parties that it had made complete disclosure of all relevant documents and attachments and that it had produced them in the ordinary manner in which they were stored by PwC. [FN83] "The only conclusion the court [could] reach [was] that PwC and/or its counsel engaged in deliberate fraud or was so recklessly indifferent to their responsibilities as a party to the litigation that they failed to take the most basic steps to fulfill those responsibilities." [FN84] The magistrate judge found that PwC's actions evidenced lack of good faith. [FN85] The judge noted that she could not recommend any sanction less than a default judgment because "PwC's conduct [had] made it impossible to try [the] case with any confidence in the justice of the outcome. . . ." [FN86] The district judge has not yet decided the issue, but the magistrate's recommended sanction is supported by precedent.

The results of our sample support the general principle that where there has been a high degree of willfulness or bad faith, a court is justified in sanctioning a party to maintain the integrity of the judicial process. [FN87] The fact-finder cannot uncover the truth when parties flout their discovery obligations and demonstrate by their conduct that they have no intention of complying with those obligations. Occasionally, however, courts have been swayed by the lack of willfulness or bad faith when they have denied sanctions. [FN88]

11 MITTLR 71
11 Mich. Telecomm. & Tech. L. Rev. 71
(Cite as: 11 Mich. Telecomm. & Tech. L. Rev. 71)

***89** C. Mixed Cases: Willfulness and Prejudice

Although our earlier discussion categorizes cases by whether courts emphasized the state of mind of the wrongdoer or the prejudice to the party seeking discovery, sanctions decisions seldom focus solely on one or the other. More often than not, both elements are involved, though one may dominate the court's discussion, as in the Thompson and Mariner cases. In cases where one or the other of these elements is less pronounced, there appears to be a sliding scale between the two. That is, the more prejudice there is, the less willfulness courts require before sanctioning a party for e-discovery violations, and vice versa. [FN89] The decisions in Mosaid Technologies Inc. v. Samsung Electronics Co., [FN90] United States v. Philip Morris USA, Inc., [FN91] and Metropolitan Opera Ass'n, Inc. v. Local 100, [FN92] are illustrative of this sliding scale.

***90** In Mosaid, a patent infringement case, the court sanctioned the defendants for, inter alia, their spoliation of technical e-mails. [FN93] The court found that defendants were required to preserve and disclose the e-mails even though Mosaid had not expressly asked for them in its document request. [FN94] Magistrate Judge Ronald Hedges reasoned that defendants "knew, or should have known, those e-mails were discoverable, given their heavy reliance on e-mails obtained from plaintiff during discovery, not to mention the obvious realities of modern litigation. . . . [T]he fact that no technical emails were preserved, and that no 'off-switch' policy existed, demonstrate[d], at the least, extremely reckless behavior." [FN95] Mosaid had made a prima facie showing of relevance through an affidavit by a former Samsung employee, testifying to the extensive and technical use of e-mail at defendants' plants. [FN96] Given the technical nature of the case, the magistrate found the prejudice to Mosaid to be "particularly obvious." [FN97] Although the magistrate imposed several sanctions for various discovery violations, he addressed defendants' spoliation of e-mails by granting an adverse inference instruction. [FN98] Mosaid proposed that the jury be instructed that it "may infer that the contents of those email messages would have been harmful to the Samsung defendants' positions in this case." [FN99] The magistrate judge rejected the proposed instruction, however, because it "fail[ed] adequately to take into account the 'make whole' aim of the adverse inference instruction. The breadth and finality of plaintiff's instruction . . . would elevate [the] e-mails to an arguably unjustified level of importance and create a potentially insurmountable hurdle for defendants." [FN100] Furthermore, plaintiff's instruction "appear[ed] on its face to deprive defendants of an opportunity to put on any evidence either in defense of their discovery failures or concerning the implication of those failures in this case." [FN101] Instead, Magistrate Judge Hedges believed Mosaid could be made whole with an instruction that permitted jurors "to infer that the evidence would have been unfavorable to defendants. In deciding whether to draw this inference, [the jurors could] consider whether these e-mails would merely have duplicated ***91** other evidence" [FN102] or whether they were "satisfied that defendants' failure to produce this information was reasonable." [FN103]

Defendants appealed the decision, and the district court affirmed. [FN104] Judge William Martini found that the spoliation inference applied because four factors had been satisfied: (1) the e-mails had been within Samsung's control since the inception of the litigation; (2) it appeared that there had been "actual suppression" or withholding of evidence; (3) the deleted e-mails were relevant to the claims or defenses in the case; and (4) it was reasonably foreseeable that technical e-mails would later be sought in discovery. [FN105] In response to Samsung's argument that the magistrate relied upon an incorrect, lower standard of culpability for "actual suppression," Judge Martini found that "negligent destruction of relevant evidence can be sufficient to give rise to the spoliation inference." [FN106] In sum, the Mosaid court required a state of mind less than willfulness, i.e., negligent or reckless, because the prejudice to plaintiff was so palpable.

By contrast, the court in United States v. Philip Morris USA, Inc., was less concerned with prejudice because Philip Morris ("PM") had shown a "reckless disregard and gross indifference" towards its discovery obligations. [FN107] In this case, PM continued deleting e-mails for two years after the court issued a preservation order. [FN108] Furthermore, after PM learned of its inadequate compliance with the order, it continued deleting e-mails for two more months and waited four months to inform the court and the government of the deletions. [FN109] If PM had complied with its own document retention policy, it would have ensured the retention of the lost e-mails. [FN110] The government moved for evidentiary and monetary sanctions for PM's spoliation of evidence. Although Judge Gladys Kessler granted sanctions, she held that the loss of e-mail records did not warrant such a far-reaching sanction as the adverse inference instruction sought by the government, i.e., an inference that the company had actively targeted youth through marketing and advertising campaigns, manipulated the nicotine content of

11 MITTLR 71
11 Mich. Telecomm. & Tech. L. Rev. 71
(Cite as: 11 Mich. Telecomm. & Tech. L. Rev. 71)

its cigarettes to make and keep smokers addicted, ***92** and failed to market potentially less hazardous cigarettes. [FN111] The requested inference was simply not proportional to the offense. However, the judge did think it was appropriate to preclude the testimony of all individuals who had failed to comply with PM's own document retention policy. [FN112] Additionally, PM was fined $2.75 million to be paid to the Court Registry as punishment for violating the preservation order. [FN113] In so holding, Judge Kessler stated:

A monetary sanction is appropriate. It is particularly appropriate here because we have no way of knowing what, if any, value those destroyed emails had to Plaintiff's case; because of that absence of knowledge, it was impossible to fashion a proportional evidentiary sanction that would accurately target the discovery violation. Despite that, it is essential that such conduct be deterred, that the corporate and legal community understand that such conduct will not be tolerated, and that the amount of the monetary sanction fully reflect the reckless disregard and gross indifference displayed by Philip Morris and [its co-defendant] toward their discovery and document preservation obligations. [FN114]

Finally, Judge Loretta Preska's decision in Metropolitan Opera Ass'n, Inc. v. Local 100 represents the furthest end of the scale, with such a high degree of willfulness that the prejudice to plaintiff was merely a secondary consideration. [FN115] The Metropolitan Opera Association ("Met") sued a restaurant-workers' union and its individual officers, alleging that the union distributed false, misleading, and defamatory materials in its attempt to unionize the Met's restaurant workers. The Met requested from the union all documents concerning the Met that were communicated or intended to be communicated to any patron, donor, board member, or agent, regarding the use or application of pressure on the Met or any of the foregoing persons, and which concerned certain events by the union. Almost from the outset, the Met's counsel began questioning the adequacy of the union's document production. At a point, it became clear that at least some electronic documents had been destroyed because the union had not understood that e-mails were called for and had not retained any electronic document or drafts. Judge Preska ***93** therefore permitted the Met to propound discovery requests concerning the union's compliance with its discovery obligations. [FN116]

It was revealed that defense counsel's behavior during discovery "was in no way 'consistent with the spirit and purposes of Rules 26 and 37.'" [FN117] "Representative examples" of the discovery abuses included: defense counsel's repeated misrepresentations to the court that all responsive documents had been produced when, in fact, a thorough search had never been made and counsel had no basis for making such representations; counsel knew the union had no document retention policy but failed to cause one to be adopted; the union delegated document production responsibilities to a non-lawyer, yet failed to explain that a document included a draft or other non-identical copy and included documents in electronic format; the non-lawyer failed to speak to all persons who might have had relevant documents, never followed up with people he did speak to, and failed to contact all of the union's internet service providers to retrieve deleted e-mails, as counsel represented he would; counsel lied to the court about a witness's vacation schedule in order to delay the witness's court-ordered deposition; and after plaintiff's counsel announced that the Met might seek to have a forensic computer expert examine the union's computers in an attempt to retrieve deleted e-mails, the union replaced their computers without notice. [FN118]

Judge Preska granted the Met's motion for sanctions and entered a default judgment against defendants "in order to (1) remedy the effect of the discovery abuses, viz., prejudicing the Met's ability to plan and prepare its case, (2) punish the parties responsible, and (3) deter similar conduct by others." [FN119] The court held that the actions of the union and its counsel rose to the level of willfulness and bad faith. [FN120] Not only had defendants made inadequate inquiries and inadequate production, but they also failed to comply with several court orders and uttered falsehoods regarding simple but material factual matters. Judge Preska concluded that lesser sanctions, such as an adverse inference or preclusion, would not be effective because there was "no indication that lesser sanctions would bring about compliance, and 'there is no meaningful way in which to correlate [defendants'] discovery failures with discrete issues in the case.'" [FN121] She adhered to her decision upon reconsideration. [FN122]

***94** IV. Conclusion

Many practitioners have expressed concern that in the absence of a safe harbor provision, courts will sanction parties for the routine recycling of electronically-stored information. They contend that the fear of sanctions will prevent businesses from adopting and implementing rational information technology systems, in which data that serves no business purpose can be deleted or otherwise destroyed. They argue that courts should be prohibited from imposing sanctions where electronic documents are lost through automatic recycling, except where the conduct was willful or reckless, or where the party violated a preservation order. In particular, defense lawyers tend to favor a safe harbor provision stronger than the one currently proposed, such as the proposal contained in the footnote accompanying proposed Rule 37(f):

A court may not impose sanctions under these rules on a party for failing to provide electronically stored information

11 MITTLR 71
11 Mich. Telecomm. & Tech. L. Rev. 71
(Cite as: 11 Mich. Telecomm. & Tech. L. Rev. 71)

deleted or lost as a result of the routine operation of the party's electronic information system unless: (1) the party intentionally or recklessly failed to preserve the information; or (2) the party violated an order issued in the action requiring the preservation of the information.

These arguments are unfounded though because they do not comport with how courts actually behave, or with principles of fundamental fairness.

First, despite ominous forecasts, the sky has not fallen in the absence of a safe harbor provision. In our sample, we did not discover a single case where a court sanctioned a party solely for following its document retention and recycling policy; there was always another consideration. Whether documents had been deleted or destroyed was not dispositive of whether courts were likely to impose e-discovery sanctions. [FN123] Courts tended to focus on the prejudice to the party seeking discovery, as well as on the spoliator's culpable state of mind. Judges did not impose sanctions for the smallest infractions, but rather, exercised their discretion to ensure that cases could be fairly adjudicated on the merits. Sometimes this meant sanctioning negligent but prejudicial conduct, and sometimes it meant denying sanctions altogether. When judges did decide to sanction e-discovery violations, willfulness played a role in the severity of the sanctions imposed. Less severe penalties, such as preclusion, were imposed for the unintentional loss of documents while the most severe sanctions (e.g., dismissal or default) were reserved for the most culpable ***95** conduct. [FN124] In no case did a judge sanction a party for the routine recycling of backup tapes where the party did not know (or should not have known) of its obligation to retain discoverable information.

Second, many of the cases in our sample did not involve intentional destruction of electronic information, and did not implicate preservation orders. If a broader safe harbor provision--such as the one quoted above--were adopted, it would hinder the courts' ability to ensure substantial justice. As previously discussed, prejudice was a significant factor in determining whether and which sanctions should be imposed. When spoliation of electronic information was prejudicial but not necessarily willful, courts asked, "How can this prejudice be overcome?" The answer ranged from the imposition of evidentiary sanctions, such as preclusion, to allowing an adverse inference to be drawn by the trier of fact. When the conduct was willful, however, the focus was no longer solely on leveling the playing field. While prejudice to the opposing party remained a powerful factor in assessing sanctions, courts also sought to punish wrongdoers. When the wrongdoer acted willfully or recklessly and the problem could not be corrected, courts have not hesitated to dismiss the complaint with prejudice or to enter default judgments. In all cases, courts were guided by notions of fairness. Any proposals to change federal or state rules of civil procedure should be similarly guided.

[FNa1]. United States District Judge for the Southern District of New York; Member of Civil Rules Advisory Committee since 1998. The opinions expressed in this Article belong to the authors alone and do not reflect the views of the Civil Rules Advisory Committee.

[FNaa1]. Law Clerk, Hon. Shira A. Scheindlin, 2004-05; Yale Law School, J.D., 2002; Duke University, B.A., 1998; Fulbright Scholar, 1998-99.

[FN1]. Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94 Civ. 2120, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995).

[FN2]. See, e.g., Thomas Y. Allman, A Preservation Safe Harbor in e-Discovery, The Antitrust Source (July 2003), available at http:// www.antitrustsource.com.

[FN3]. See infra notes 33-35.

[FN4]. Report of the Civil Rules Advisory Committee 17 (Aug. 3, 2004), available at http://www.uscourts.gov/rules/comment2005/CVAug04.pdf.

[FN5]. Proposed Amendments to the Federal Rules of Civil Procedure 32 (proposed Aug. 3, 2004), available at http:// www.uscourts.gov/rules/comment2005/CVAug04.pdf.

[FN6]. Id. at 31-32.

[FN7]. E.g., Mike France, Taking the Fear Factor Out of E-Mail, BusinessWeek (Dec. 20, 2004).

11 MITTLR 71
11 Mich. Telecomm. & Tech. L. Rev. 71
(Cite as: 11 Mich. Telecomm. & Tech. L. Rev. 71)

[FN8]. Although strictly speaking the twenty-first century (and third millennium) began on January 1, 2001, we used January 1, 2000, as our starting date based on the colloquial use of the term "twenty-first century" and on the desirability of having a larger sample size.

[FN9]. We did not include Rambus, Inc. v. Infineon Technologies, 220 F.R.D. 264 (E.D. Va. 2004), in our sample because the various decisions did not reveal whether the alleged spoliation covered electronic as well as paper records. But because the case has been frequently cited in e-discovery circles it makes sense to summarize its holding in this article. In Rambus, the defendant filed a motion to compel the production of documents and testimony relating to the plaintiff's document retention policy because the plaintiff allegedly destroyed documents when it knew or should have known of the impending patent infringement action. Defendants cited to plaintiff's e-mails as proof that the plaintiff engaged in a "Shred Day," in which its employees shredded approximately two million pages of documents, including evidence related to the pending patent infringement case. The plaintiff admitted that its document purging system was adopted due to discovery-related concerns but denied that it was trying to keep unfavorable information from its adversaries. The plaintiff argued that it had accumulated too much information, including back up tapes, which would involve huge search and review costs in any future litigation. The court held that even if the plaintiff had not instituted its document retention policy in bad faith, it would be guilty of spoliation if it reasonably anticipated litigation when it implemented the policy.

In a later opinion, the court held that defendant had made a prima facie showing that the plaintiff intentionally engaged in spoliation of evidence and that the crime fraud exception should operate to pierce the attorney-client privilege. See Rambus, 222 F.R.D. 280 (E.D. Va. 2004). The court granted defendant discovery for the purpose of making a presentation to the court as to what the appropriate sanction should be.

[FN10]. See Rowe v. Albertsons, Inc., No. 02-4186, 2004 WL 2252064 (10th Cir. Oct. 7, 2004); Computer Task Group, Inc. v. Brotby, 364 F.3d 1112 (9th Cir. 2004); Morris v. Union Pac. R.R. Co., 373 F.3d 896 (8th Cir. 2004); Stevenson v. Union Pac. R.R. Co., 354 F.3d 739 (8th Cir. 2004); United States v. Philip Morris USA, Inc., 327 F. Supp. 2d 21 (D.D.C. 2004); Metropolitan Opera Ass'n. v. Local 100, 212 F.R.D. 178 (S.D.N.Y. 2003); Cobell v. Norton, 206 F.R.D. 324 (D.D.C. 2002); Filanowski v. Wal-Mart Stores, Inc., No. Civ. 99-147-B-H, 2000 WL 761890 (D. Me. Apr. 6, 2000); GTFM, Inc. v. Wal-Mart Stores, Inc., No. 98 Civ. 7724, 2000 WL 335558 (S.D.N.Y. Mar. 30, 2000); Tomlin v. Wal-Mart Stores, Inc., 100 S.W.3d 57 (Ark. Ct. App. Mar. 12, 2003); Mariner Health Care, Inc. v. PriceWaterhouseCoopers LLP, No. 02VS037631-F, slip op. (Ga. Fulton Cty. Nov. 9, 2004); Bandy v. Cincinnati, New Orleans and Tex. Pac. Ry. Co., No. 2001-CA-002121, 2003 WL 22319202 (Ky. Ct. App. Oct. 10, 2003); Wadja v. Kingsbury, 652 N.W.2d 856 (Minn. Ct. App. 2002); Playball at Hauppauge, Inc. v. Narotzky, 745 N.Y.S.2d 70 (N.Y. Ct. App. 2002); Eichman v. McKeon, 824 A.2d 305 (Pa. Super. 2003); Demelash v. Ross Stores, Inc., 20 P.3d 447 (Wash. Ct. App. 2001).

[FN11]. See Inst. for Motivational Living, Inc. v. Doulos Inst. for Strategic Consulting, Inc., No. 03-4177, 2004 WL 2241745 (3d Cir. Oct. 5, 2004); Minn. Mining & Mfg. v. Pribyl, 259 F.3d 587 (7th Cir. 2001); Advantacare Health Partners v. Access IV, No. C 03-04496, 2004 WL 1837997 (N.D. Cal. Aug. 17, 2004); Mosaid Techs. Inc. v. Samsung Elecs. Co., No. 01 CV 4340, 2004 U.S. Dist. LEXIS 23596 (D.N.J. July 7, 2004); MasterCard Int'l, Inc. v. Moulton, No. 03 Civ. 3613, 2004 WL 1393992 (S.D.N.Y. June 22, 2004); Aero Prods. Int'l v. Intex Recreation Corp., No. 02 C 2590, 2004 WL 417193 (N.D. Ill. Jan. 30, 2004); Arista Records, Inc. v. Sakfield Holding Co. S.L., 314 F. Supp. 2d 27 (D.D.C. 2004); Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162 (S.D.N.Y. 2004); Liafail, Inc. v. Learning 2000, Inc., No. C.A. 01-599, 2002 WL 31954396 (D. Del. Dec. 23, 2003); Kucala Enters., Ltd. v. Auto Wax Co., Inc., No. 02 C 1403, 2003 WL 22433095 (N.D. Ill. May 27, 2003); Essex Group v. Express Wire Servs., 578 S.E.2d 705 (N.C. Ct. App. 2003); Hildreth Mfg., LLC v. Semco, Inc., 785 N.E.2d 774 (Ohio Ct. App. 2003); QZO, Inc. v. Moyer, 594 S.E.2d 541 (S.C. Ct. App. 2004).

[FN12]. See Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99 (2d Cir. 2002); Lyondell-Citgo Ref., L.P. v. Petroleos de Venezuela, S.A., No. 02 Civ. 0795, 2004 WL 1924810 (S.D.N.Y. Aug. 30, 2004); YCA, LLC v. Berry, No. 03 C 3116, 2004 WL 1093385 (N.D. Ill. May 7, 2004); Invision Media Communications, Inc. v. Fed. Ins. Co., No. 02 Civ. 5461, 2004 WL 396037 (S.D.N.Y. Mar. 2, 2004); Network Computing Servs. Corp. v. Cisco Sys., Inc., 223 F.R.D. 392 (D.S.C. 2004); Renda Marine, Inc. v. United States, No. 02- 306, 58 Fed. Cl. 57 (2003); Pennar Software Corp. v. Fortune 500 Sys. Ltd., No. 01-01734, 2001 U.S. Dist. LEXIS 18432 (N.D. Cal. Oct. 25, 2001); Feather River Anesthesia Med. Group, Inc. v. Fremont-Rideout Health Group, No. C044559, 2004 WL 1468741 (Cal. Ct. App. June 30, 2004); Montage Group, Ltd. v. Athle-Tech Computer Sys., Inc., No. 2D03-2026, 2004 WL 2892394 (Fla. Ct. App. Oct. 13, 2004); Munshani v. Signal Lake Venture Fund II, 805 N.E.2d 998 (Mass. App. Ct. Mar. 26, 2004); Nartron Corp. v. Gen'l Motors Corp., No. 232085, 2003 WL 1985261 (Mich. Ct. App. Apr. 29, 2003); Long Island Diagnostic Imaging v. Stony Brook Diagnostic Assocs., 286 A.D.2d 320 (N.Y. Ct. App. 2001).

11 MITTLR 71
11 Mich. Telecomm. & Tech. L. Rev. 71
(Cite as: 11 Mich. Telecomm. & Tech. L. Rev. 71)

[FN13]. See Zubulake v. UBS Warburg, LLC, No. 02 Civ. 1243, 2004 WL 1620866 (S.D.N.Y. July 20, 2004) ("Zubulake V"); Anderson v. Crossroads Capital Partners, LLC, No. Civ. 01-2000, 2004 WL 256512 (D. Minn. Feb. 10, 2004); Wiginton v. Ellis, No. 02 C 6832, 2003 WL 22439865 (N.D. Ill. Oct. 27, 2003); Sonii v. Gen. Elec. Corp., No. 95 C 5370, 2003 WL 21541039 (N.D. Ill. June 11, 2003); Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212 (S.D.N.Y. 2003) ("Zubulake IV"); Kormendi v. Computer Assocs. Int'l, No. 02 Civ. 2996, 2002 WL 31385832 (S.D.N.Y. Oct. 21, 2002); Williams v. Saint-Gobain Corp., No. 00-CV-0502E, 2002 WL 1477618 (W.D.N.Y. June 28, 2002); Sheppard v. River Valley Fitness One, L.P., 203 F.R.D. 56 (D.N.H. 2001); Lombardo v. Broadway Stores, Inc., No. G026581, 2002 WL 86810 (Cal. Ct. App. Jan. 22, 2002); Comm'r of Labor v. Ward, 580 S.E.2d 432 (N.C. Ct. App. 2003).

[FN14]. See Beck v. Haik, 377 F.3d 624 (6th Cir. 2004) (civil rights); In re Heritage Bond Litig., 223 F.R.D. 527 (C.D. Cal. 2004) (commercial); Williams v. Ehlenz, No. Civ. 02-978, 2004 WL 742076 (D. Minn. Mar. 30, 2004) (civil rights); Keir v. UnumProvident, No. 02 Civ. 8781, 2003 WL 21997747 (S.D.N.Y. Aug. 22, 2003) (ERISA); Landmark Legal Found. v. EPA, 272 F. Supp. 2d 70 (D.D.C. 2003) (FOIA); Thompson v. United States Dep't of Hous. and Urban Dev., 219 F.R.D. 93 (D. Md. 2003) (modification of consent decree to desegregate public housing); DeLoach v. Philip Morris Co., 206 F.R.D. 568 (M.D.N.C. 2002) (antitrust); Trigon Ins. Co. v. United States, 234 F. Supp. 2d 592 (E.D. Va. 2002) (tax refund action); United States v. Murphy Oil USA, Inc., 155 F. Supp. 2d 1117 (W.D. Wis. 2001) (environmental); W.R. Grace & Co.-Conn. v. Zotos Int'l, Inc., No. 98-CV-838S, 2000 WL 1843258 (W.D.N.Y. Nov. 2, 2000) (contribution for CERCLA response costs); Danis v. USN Communications, No. 98 C 7482, 2000 WL 1694325 (N.D. Ill. Oct. 23, 2000) (securities); Sieferman v. State Farm Mut. Auto. Ins. Co., 796 So.2d 833 (La. Ct. App. 2001) (insurance coverage); Thomas v. Isle of Capri Casino, 781 So.2d 125 (Miss. 2001) (challenge of Gaming Commission decision); Crescendo Invs., Inc. v. Brice, 61 S.W.3d 465 (Tex. App. 2001) (securities); Yao v. Bd. of Regents of Univ. of Wis. Sys., 649 N.W.2d 356 (Wis. Ct. App. 2002) (appealing Board of Regents action).

[FN15]. See infra notes 16-17.

[FN16]. See Inst. Motivational Living, 2004 WL 2241745; Computer Task Group, Inc. v. Brotby, 364 F.3d 1112 (9th Cir. 2004); Stevenson v. Union Pac. R.R. Co., 354 F.3d 739 (8th Cir. 2004); Minn. Mining, 259 F.3d 587; Advantacare, 2004 WL 1837997; Zubulake V, 2004 WL 1620866; Mosaid, 2004 U.S. Dist. LEXIS 23596; MasterCard, 2004 WL 1393992; United States v. Philip Morris USA, Inc., 327 F. Supp. 2d 21 (D.D.C. 2004); In re Heritage Bond Litig., 223 F.R.D. 527; Sonii, 2003 WL 21541039; Landmark Legal, 272 F. Supp. 2d 70; Zubulake IV, 220 F.R.D. 212; Thompson, 219 F.R.D. 93; Renda, 58 Fed. Cl. 57; Metropolitan Opera Ass'n. v. Local 100, 212 F.R.D. 178 (S.D.N.Y. 2003); DeLoach, 206 F.R.D. 568; Cobell v. Norton, 206 F.R.D. 324 (D.D.C. 2002); Pennar, 2001 U.S. Dist. LEXIS 18432; Trigon, 234 F. Supp. 2d 592; Sheppard, 203 F.R.D. 56; W.R. Grace, 2000 WL 1843258; Danis, 2000 WL 1694325; GTFM, Inc. v. Wal-Mart Stores, Inc., No. 98 Civ. 7724, 2000 WL 335558 (S.D.N.Y. Mar. 30, 2000); Feather River, 2004 WL 1468741; Lombardo, 2002 WL 86810; Montage, 2004 WL 2892394; Bandy v. Cincinnati, New Orleans and Tex. Pac. Ry. Co., No. 2001-CA-002121, 2003 WL 22319202 (Ky. Ct. App. Oct. 10, 2003); Sieferman, 796 So.2d 833; Wadja v. Kingsbury, 652 N.W.2d 856 (Minn. Ct. App. 2002); Isle of Capri, 781 So.2d 125; Long Island, 286 A.D.2d 320; Ward, 580 S.E.2d 432; Essex Group, 578 S.E.2d 705; QZO, 594 S.E.2d 541.

[FN17]. See Invision Media, 2004 WL 396037; Anderson, 2004 WL 256212; Network Computing, 223 F.R.D. 392 (D.S.C. 2004); Kucala Enters., Ltd. v. Auto Wax Co., Inc., No. 02 C 1403, 2003 WL 22433095 (N.D. Ill. May 27, 2003); Mariner Health Care, Inc. v. PriceWaterhouseCoopers LLP, No. 02VS037631-F, slip op. (Ga. Fulton Cty. Nov. 9, 2004); Munshani, 805 N.E.2d 998; Nartron, 2003 WL 1985261; Playball at Hauppauge, Inc. v. Narotzky, 745 N.Y.S.2d 70 (N.Y. Ct. App. 2002).

[FN18]. See Inst. for Motivational Living, 2004 WL 2241745; Computer Task, 364 F.3d 1112; Stevenson, 354 F.3d 739; Minn. Mining, 259 F.3d 587; Advantacare, 2004 WL 1837997; Zubulake V, 2004 WL 1620866; Mosaid, 2004 U.S. Dist. LEXIS 23596; MasterCard, 2004 WL 1393992; Anderson, 2004 WL 256512; Philip Morris, 327 F. Supp. 2d 21; In re Heritage Bond Litig., 223 F.R.D. 527; Kucala, 2003 WL 22433095; Landmark Legal, 272 F. Supp. 2d 70; Zubulake IV, 220 F.R.D. 212; Thompson, 219 F.R.D. 93; Metropolitan Opera, 212 F.R.D. 178; Renda, 58 Fed. Cl. 57; Pennar, 2001 U.S. Dist. LEXIS 18432; Trigon, 234 F. Supp. 2d 592; Sheppard, 203 F.R.D. 56; W.R.Grace, 2000 WL 1843258; Danis, 2000 WL 1694325; GTFM, 2000 WL 335558; Lombardo, 2002 WL 86810; Montage, 2004 WL 2289569; Bandy, 2003 WL 22319202; Sieferman, 796 So.2d 833; Nartron, 2003 WL 1985261; Wadja, 652 N.W.2d 856; Isle of Capri, 781 So.2d 125; Long Island, 286 A.D.2d 320; Playball, 745 N.Y.S.2d 70; Ward, 580 S.E.2d 705; Essex, 578 S.E.2d 705; QZO, 594 S.E.2d 541.

[FN19]. See Invision Media, 2004 WL 396037; Network Computing, 223 F.R.D. 392; Sonii, 2003 WL 21541039; DeLoach, 206 F.R.D. 568; Cobell, 206 F.R.D. 324; Feather River, 2004 WL 1468741; Mariner, No. 02VS037631- F, slip op.

[FN20]. See Invision Media, 2004 WL 396037 (representing falsely the existence and location of relevant documents); Network Computing, 223 F.R.D. 392 (producing e-mails after repeatedly telling magistrate judge that they did not exist); Mariner, No. 02VS037631-F, slip op. (assuring court that plaintiff could make production deadlines in compliance with court orders when plaintiff knew it could or would not).

[FN21]. See infra notes 22-24.

[FN22]. See Inst. for Motivational Living, 2004 WL 2241745; Philip Morris, 327 F. Supp. 2d 21; Kucala, 2003 WL 22433095; Landmark Legal, 272 F. Supp. 2d 70; Metropolitan Opera, 212 F.R.D. 178; Renda, 58 Fed. Cl. 57; Danis, 2000 WL 1694325.

[FN23]. See Computer Task, 364 F.3d 1112; Anderson, 2004 WL 256512; In re Heritage Bond Litig., 223 F.R.D. 527; Network Computing, 223 F.R.D. 392; Thompson, 219 F.R.D. 93; Sheppard, 203 F.R.D. 56; Feather River, 2004 WL 1468741; Montage, 2004 WL 2892394; Mariner, No. 02VS037631-F, slip op.; Sieferman, 796 So.2d 833; Nartron, 2003 WL 1985261; Long Island, 286 A.D.2d 320; Ward, 580 S.E.2d 432.

[FN24]. See Minn. Mining & Mfg. v. Pribyl, 259 F.3d 587 (7th Cir. 2001); Advantacare Health Partners v. Access IV, No. C 03-04496, 2004 WL 1837997 (N.D. Cal. Aug. 17, 2004); QZO, Inc. v. Moyer, 594 S.E.2d 541 (S.C. Ct. App. 2004).

[FN25]. See Inst. for Motivational Living, 2004 WL 2241745; Computer Task, 364 F.3d 1112; Stevenson v. Union Pac. R.R. Co., 354 F.3d 739 (8th Cir. 2004); Minn. Mining, 259 F.3d 587; Advantacare, 2004 WL 1837997; Zubulake v. UBS Warburg, LLC, No. 02 Civ. 1243, 2004 WL 1620866 (S.D.N.Y. July 20, 2004); Invision Media, 2004 WL 396037; Anderson, 2004 WL 256512; In re Heritage Bond Litig., 223 F.R.D. 527; Network Computing, 223 F.R.D. 392; Kucala, 2003 WL 22433095; Cobell v. Norton, 206 F.R.D. 324 (D.D.C. 2002); Pennar Software Corp. v. Fortune 500 Sys. Ltd., No. 01- 01734, 2001 U.S. Dist. LEXIS 18432 (N.D. Cal. Oct. 25, 2001); Trigon Ins. Co. v. United States, 204 F.R.D. 277 (E.D.Va. 2001); Lombardo v. Broadway Stores, Inc., No. G026581, 2002 WL 86810 (Cal. Ct. App. Jan. 22, 2002); Montage, 2004 WL 2892394; Mariner, No. 02VS037631-F, slip op.; Bandy v. Cincinnati, New Orleans and Tex. Pac. Ry. Co., No. 2001-CA-002121, 2003 WL 22319202 (Ky. Ct. App. Oct. 10, 2003); Munshani v. Signal Lake Venture Fund II, 805 N.E.2d 998 (Mass. App. Ct. Mar. 26, 2004); Ward, 580 S.E.2d 432; QZO, 594 S.E.2d 541.

[FN26]. See Computer Task, 364 F.3d 1112; Stevenson, 354 F.3d 739; Advantacare, 2004 WL 1837997; Zubulake V, 2004 WL 1620866; Mosaid Techs. Inc. v. Samsung Elecs. Co., No. 01 CV 4340, 2004 U.S. Dist. LEXIS 23596 (D.N.J. July 7, 2004); In re Heritage Bond Litig., 223 F.R.D. 527; Thompson, 219 F.R.D. 93; DeLoach v. Philip Morris Co., 206 F.R.D. 568 (M.D.N.C. 2002); Trigon, 204 F.R.D. 277; Sheppard, 203 F.R.D. 56; W.R. Grace & Co.-Conn. v. Zotos Int'l, Inc., No. 98-CV-838S, 2000 WL 1843258 (W.D.N.Y. Nov. 2, 2000); Mariner, No. 02VS037631-F, slip op.; Wadja v. Kingsbury, 652 N.W.2d 856 (Minn. Ct. App. 2002); Thomas v. Isle of Capri Casino, 781 So.2d 125 (Miss. 2001); Playball at Hauppauge, Inc. v. Narotzky, 745 N.Y.S.2d 70 (N.Y. Ct. App. 2002).

[FN27]. See MasterCard Int'l, Inc. v. Moulton, No. 03 Civ. 3613, 2004 WL 1393992 (S.D.N.Y. June 22, 2004); Philip Morris, 327 F. Supp. 2d 21; Sonii v. Gen. Elec. Corp., No. 95 C 5370, 2003 WL 21541039 (N.D. Ill. June 11, 2003); Isle of Capri, 781 So.2d 125.

[FN28]. See Inst. for Motivational Living, 2004 WL 2241745; Computer Task, 364 F.3d 1112; Stevenson, 354 F.3d 739; Advantacare, 2004 WL 1837997; Zubulake V, 2004 WL 1620866; Mosaid, 2004 U.S. Dist. LEXIS 23596; Invision Media, 2004 WL 396037; Anderson, 2004 WL 256512; In re Heritage Bond Litig., 223 F.R.D. 527; Philip Morris, 327 F. Supp. 2d 21; Sonii, 2003 WL 21541039; Kucala, 2003 WL 22433095; Landmark Legal Found. v. EPA, 272 F. Supp. 2d 70 (D.D.C. 2003); Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212 (S.D.N.Y. 2003) ("Zubulake IV"); Thompson, 219 F.R.D. 93; Metropolitan Opera Ass'n. v. Local 100, 212 F.R.D. 178 (S.D.N.Y. 2003); Renda Marine, Inc. v. United States, No. 02-306, 58 Fed. Cl. 57 (2003); Cobell, 206 F.R.D. 324; Pennar, 2001 U.S. Dist. LEXIS 18432; Trigon, 204 F.R.D. 277; Sheppard, 203 F.R.D. 56; W.R. Grace, 2000 WL 1843258; Danis v. USN Communications, No. 98 C 7482, 2000 WL 1694325 (N.D. Ill. Oct. 23, 2000); GTFM, Inc. v. Wal-Mart Stores, Inc., No. 98 Civ. 7724, 2000 WL 335558 (S.D.N.Y. Mar. 30, 2000);

11 MITTLR 71
11 Mich. Telecomm. & Tech. L. Rev. 71
(Cite as: 11 Mich. Telecomm. & Tech. L. Rev. 71)

Feather River, 2004 WL 1468741; Lombardo, 2002 WL 86810; Essex Group v. Express Wire Servs., 578 S.E.2d 705 (N.C. Ct. App. 2003).

[FN29]. See Advantacare, 2004 WL 1837997; Mosaid, 2004 U.S. Dist. LEXIS 23596; In re Heritage Bond Litig., 223 F.R.D. 527; Network Computing, 223 F.R.D. 392; Philip Morris, 327 F. Supp. 2d 21; Kucala, 2003 WL 22433095; Thompson, 219 F.R.D. 93; DeLoach, 206 F.R.D. 568; Sheppard, 203 F.R.D. 56; Montage, 2004 WL 2892394; Sieferman v. State Farm Mut. Auto. Ins. Co., 796 So.2d 833 (La. Ct. App. 2001); Ward, 580 S.E.2d 432; Essex, 578 S.E.2d 705.

[FN30]. See Stevenson, 354 F.3d 739; Minn. Mining, 259 F.3d 587; Zubulake V, 2004 WL 1620866; Mosaid, 2004 U.S. Dist. LEXIS 23596; MasterCard, 2004 WL 1393992; Anderson, 2004 WL 256512; Trigon, 204 F.R.D. 277; Bandy, 2003 WL 22319202; Wadja, 652 N.W.2d 856; Isle of Capri, 781 So.2d 125.

[FN31]. See Computer Task, 364 F.3d 1112; Metropolitan Opera, 212 F.R.D. 178; Mariner, No. 02VS037631-F, slip op.; Munshani v. Signal Lake Venture Fund II, 805 N.E.2d 998 (Mass. App. Ct. Mar. 26, 2004); Nartron Corp. v. Gen'l Motors Corp., No. 232085, 2003 WL 1985261 (Mich. Ct. App. Apr. 29, 2003); Long Island Diagnostic Imaging v. Stony Brook Diagnostic Assocs., 286 A.D.2d 320 (N.Y. Ct. App. 2001); Playball, 745 N.Y.S.2d 70; Ward, 580 S.E.2d 432; Essex, 578 S.E.2d 705; QZO, Inc. v. Moyer, 594 S.E.2d 541 (S.C. Ct. App. 2004).

[FN32]. See Stevenson, 354 F.3d 739 (adverse inference, monetary); Advantacare, 2004 WL 1837997 (evidentiary, monetary); Zubulake V, 2004 WL 1620866 (adverse inference, monetary); Mosaid, 2004 U.S. Dist. LEXIS 23596 (evidentiary, adverse inference, monetary); Anderson, 2004 WL 256512 (adverse inference, monetary); In re Heritage Bond Litig., 223 F.R.D. 527 (evidentiary, monetary); Philip Morris, 327 F. Supp. 2d 21 (evidentiary, monetary); Kucala, 2003 WL 22433095 (evidentiary, monetary); Thompson, 219 F.R.D. 93 (evidentiary, monetary); Metropolitan Opera, 212 F.R.D. 178 (default judgment, monetary); Trigon, 204 F.R.D. 277 (adverse inference, monetary) Sheppard, 203 F.R.D. 56 (evidentiary, monetary); Essex, 578 S.E.2d 705 (default judgment, evidentiary, monetary).

[FN33]. See Computer Task, 364 F.3d 1112; Zubulake V, 2004 WL 1620866; Mosaid, 2004 U.S. Dist. LEXIS 23596; Invision Media, 2004 WL 396037; In re Heritage Bond Litig., 223 F.R.D. 527; Network Computing,223 F.R.D. 392; Sonii, 2003 WL 21541039; Kucala, 2003 WL 22433095; Zubulake IV, 220 F.R.D. 212; Thompson, 219 F.R.D. 93; Metropolitan Opera, 212 F.R.D. 178; Pennar, 2001 U.S. Dist. LEXIS 18432; Sheppard, 203 F.R.D. 56; W.R. Grace, 2000 WL 1843258; Danis, 2000 WL 1694325; GTFM, 2000 WL 335558.

[FN34]. See Lombardo v. Broadway Stores, Inc., No. G026581, 2002 WL 86810 (Cal. Ct. App. Jan. 22, 2002); Mariner, No. 02VS037631-F, slip op.; Sieferman, 796 So.2d 833; Nartron, 2003 WL 1985261; Ward, 580 S.E.2d 432; Essex, 578 S.E.2d 705.

[FN35]. See Advantacare, 2004 WL 1837997; Mosaid, 2004 U.S. Dist. LEXIS 23596; Invision Media, 2004 WL 396037; Anderson, 2004 WL 256512; Sonii, 2003 WL 21541039; Zubulake IV, 220 F.R.D. 212; Trigon, 204 F.R.D. 277; Landmark Legal Found. v. EPA, 272 F. Supp. 2d 70 (D.D.C. 2003); Pennar, 2001 U.S. Dist. LEXIS 18432; Mariner, No. 02VS037631-F, slip op.; Munshani, 805 N.E.2d 998; Wadja, 652 N.W.2d 856.

[FN36]. See Stevenson, 354 F.3d 739; Inst. for Motivational Living, Inc. v. Doulos Inst. for Strategic Consulting, Inc., No. 03-4177, 2004 WL 2241745 (3d Cir. Oct. 5, 2004); Minn. Mining & Mfg. v. Pribyl, 259 F.3d 587 (7th Cir. 2001); MasterCard Int'l, Inc. v. Moulton, No. 03 Civ. 3613, 2004 WL 1393992 (S.D.N.Y. June 22, 2004); Philip Morris, 327 F. Supp. 2d 21; Renda Marine, Inc. v. United States, No. 02-306, 58 Fed. Cl. 57 (2003); DeLoach v. Philip Morris Co., 206 F.R.D. 568 (M.D.N.C. 2002); Cobell v. Norton, 206 F.R.D. 324 (D.D.C. 2002); Feather River Anesthesia Med. Group, Inc. v. Fremont-Rideout Health Group, No. C044559, 2004 WL 1468741 (Cal. Ct. App. June 30, 2004); Montage Group, Ltd. v. Athle-Tech Computer Sys., Inc., No. 2D03-2026, 2004 WL 2892394 (Fla. Ct. App. Oct. 13, 2004); Bandy v. Cincinnati, New Orleans and Tex. Pac. Ry. Co., No. 2001-CA-002121, 2003 WL 22319202 (Ky. Ct. App. Oct. 10, 2003); Wadja, 652 N.W.2d 856; Thomas v. Isle of Capri Casino, 781 So.2d 125 (Miss. 2001); Long Island, 286 A.D.2d 320; Playball, 745 N.Y.S.2d 70; QZO, 594 S.E.2d 541.

[FN37]. See Rowe v. Albertsons, Inc., No. 02-4186, 2004 WL 2252064 (10th Cir. Oct. 7, 2004); Beck v. Haik, 377 F.3d 624 (6th Cir. 2004); Morris v. Union Pac. R.R. Co., 373 F.3d 896 (8th Cir. 2004); Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99 (2d Cir. 2002); Lyondell-Citgo Ref., L.P. v. Petroleos de Venezuela, S.A., No. 02 Civ. 0795, 2004 WL

1924810 (S.D.N.Y. Aug. 30, 2004); Arista Records, Inc. v. Sakfield Holding Co. S.L., 314 F. Supp. 2d 27 (D.D.C. 2004); Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162 (S.D.N.Y. 2004); YCA, LLC v. Berry, No. 03 C 3116, 2004 WL 1093385 (N.D. Ill. May 7, 2004); Williams v. Ehlenz, No. Civ. 02-978, 2004 WL 742076 (D. Minn. Mar. 30, 2004); Aero Prods. Int'l v. Intex Recreation Corp., No. 02 C 2590, 2004 WL 417193 (N.D. Ill. Jan. 30, 2004); Liafail, Inc. v. Learning 2000, Inc., No. C.A. 01-599, 2002 WL 31954396 (D. Del. Dec. 23, 2003); Wiginton v. Ellis, No. 02 C 6832, 2003 WL 22439865 (N.D. Ill. Oct. 27, 2003); Keir v. UnumProvident, No. 02 Civ. 8781, 2003 WL 21997747 (S.D.N.Y. Aug. 22, 2003); Kormendi v. Computer Assocs. Int'l, No. 02 Civ. 2996, 2002 WL 31385832 (S.D.N.Y. Oct. 21, 2002); Williams v. Saint-Gobain Corp., No. 00-CV-0502E, 2002 WL 1477618 (W.D.N.Y. June 28, 2002); United States v. Murphy Oil USA, Inc., 155 F. Supp. 2d 1117 (W.D. Wis. 2001); Filanowski v. Wal-Mart Stores, Inc., No. Civ. 99-147-B-H, 2000 WL 761890 (D. Me. Apr. 6, 2000); Tomlin v. Wal-Mart Stores, Inc., 100 S.W.3d 57 (Ark. Ct. App. Mar. 12, 2003); Hildreth Mfg., LLC v. Semco, Inc., 785 N.E.2d 774 (Ohio Ct. App. 2003); Eichman v. McKeon, 824 A.2d 305 (Pa. Super. 2003); Yao v. Bd. of Regents of Univ. of Wis. Sys., 649 N.W.2d 356 (Wis. Ct. App. 2002); Crescendo Invs., Inc. v. Brice, 61 S.W.3d 465 (Tex. App. 2001); Demelash v. Ross Stores, Inc., 20 P.3d 447 (Wash. Ct. App. 2001).

[FN38]. See Rowe, 2004 WL 2252064; Beck, 377 F.3d 624; Morris, 373 F.3d 896; Residential Funding, 306 F.3d 99; Arista Records, 314 F. Supp. 2d 27; Convolve, 223 F.R.D. 162; Ehlenz, 2004 WL 742076; Aero Prods., 2004 WL 417193; Liafail, 2002 WL 31954396; Wiginton, 2003 WL 22439865; Keir, 2003 WL 21997747; Kormendi, 2002 WL 31385832; Murphy Oil, 155 F. Supp. 2d 1117; Filanowski, 2000 WL 761890; Tomlin, 100 S.W.3d 57; Hildreth, 785 N.E.2d 774; Eichman, 824 A.2d 305; Yao, 649 N.W.2d 356; Crescendo, 61 S.W.3d 465; Demelash, 20 P.3d 447.

[FN39]. See Lyondell, 2004 WL 1924810; Arista Records, 314 F. Supp. 2d 27; Aero Prods., 2004 WL 417193; Wiginton, 2003 WL 22439865; Keir, 2003 WL 21997747; Kormendi, 2002 WL 31385832; St.-Gobain, 2002 WL 1477618; Hildreth, 785 N.E.2d 774; Demelash, 20 P.3d 447.

[FN40]. See infra note 44.

[FN41]. See Rowe, 2004 WL 2252064 (reversing grant of summary judgment to defendant so that district court could consider the appropriateness of imposing spoliation presumption, which it had not considered in the first instance); Beck, 377 F.3d 624 (reversing judgment in favor of defendants because, inter alia, exclusion of evidence of defendants' spoliation of evidence was abuse of discretion); Residential Funding, 306 F.3d 99 (reversing district court's denial of adverse inference instruction because court used wrong standard for culpable state of mind); Demelash, 20 P.3d 447 (reversing judgment because it was based on erroneous conclusion that defendant need not produce evidence essential to plaintiff's case).

[FN42]. See Morris, 373 F.3d 896; Convolve, 223 F.R.D. 162; Ehlenz, 2004 WL 742076; St.-Gobain, 2002 WL 1477618; Murphy Oil, 155 F. Supp. 2d 117; Eichman, 824 A.2d 305; Yao, 649 N.W.2d 356; Crescendo, 61 S.W.3d 465.

[FN43]. See YCA, LLC v. Berry, No. 03 C 3116, 2004 WL 1093385 (N.D. Ill. May 7, 2004); Convolve, 223 F.R.D. 162; Wiginton, 2003 WL 22439865; St.-Gobain, 2002 WL 1477618; Tomlin, 100 S.W.3d 57 Hildreth, 785 N.E.2d 774; Eichman, 824 A.2d 305.

[FN44]. See Arista Records, 314 F. Supp. 2d 27; Keir, 2003 WL 21997747; Liafail, Inc. v. Learning 2000, Inc., No. C.A. 01-599, 2002 WL 31954396 (D. Del. Dec. 23, 2003); Kormendi, 2002 WL 31385832.

[FN45]. See Lyondell-Citgo Ref., L.P. v. Petroleos de Venezuela, S.A., No. 02 Civ. 0795, 2004 WL 1924810 (S.D.N.Y. Aug. 30, 2004) (noting that the attorney general of Venezuela had issued directive to defendants not to produce electronic data, contending that the files related to a sabotage investigation); Aero Prods. Int'l v. Intex Recreation Corp., No. 02 C 2590, 2004 WL 417193 (N.D. Ill. Jan. 30, 2004) (noting that plaintiff had not filed a petition, as was its right to do, under the discovery order, seeking the appointment of a computer forensics expert to assist in recovering data); Filanowski v. Wal-Mart Stores, Inc., No. Civ. 99-147-B-H, 2000 WL 761890 (D. Me. Apr. 6, 2000) (failing to recognize a cause of action for spoliation of evidence).

[FN46]. See Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 750 (8th Cir. 2004) ("Sanctioning the ongoing destruction of records during litigation and discovery by imposing an adverse inference instruction is supported by either the court's inherent power or Rule 37 of the Federal Rules of Civil Procedure, even absent an explicit bad faith finding, and we conclude that the giving of an adverse inference instruction in these circumstances is not an abuse of discretion."); Young v. Gordon,

11 MITTLR 71
11 Mich. Telecomm. & Tech. L. Rev. 71
(Cite as: 11 Mich. Telecomm. & Tech. L. Rev. 71)

330 F.3d 76, 82 (1st Cir. 2003) ("[A] finding of bad faith is not a condition precedent to imposing a sanction of dismissal."); Residential Funding, 306 F.3d at 113 ("In sum, we hold that ... discovery sanctions [under Rule 37], including an adverse inference instruction, may be imposed upon a party that has breached a discovery obligation not only through bad faith or gross negligence, but also through ordinary negligence."); Yeti by Molly, Ltd. v. Deckers Outdoor Corp., 259 F.3d 1101, 1106 (9th Cir. 2001) (finding of willfulness, bad faith, or fault not required for entry of sanctions less than a dismissal); Melendez v. Illinois Bell Telephone Co., 79 F.3d 661, 671 (7th Cir. 1996) ("Bad faith ... is not required for a district court to sanction a party for discovery abuses."); Vodusek v. Bayliner Marine Corp., 71 F.3d 148, 156 (4th Cir. 1995) ("While a finding of bad faith suffices to permit such an [adverse] inference, it is not always necessary."); Bank Atlantic v. Blythe Eastman Paine Webber, Inc., 12 F.3d 1045, 1049 (11th Cir. 1994) (holding that bad faith or willfulness not required for entry of discovery sanctions less than default or dismissal); Turnbull v. Wilcken, 893 F.2d 256, 259 (10th Cir. 1990) (noting that sanction of attorney's fees and costs permitted even where there is an absence of bad faith); Regional Refuse Sys., Inc. v. Inland Reclam. Co., 842 F.2d 150, 156 (6th Cir. 1988), overruled on other grounds as superceded by rule change; Vance, by and through Hammons v. United States, 182 F.3d 920 (6th Cir. 1999) (holding that where a party has the ability to comply with a discovery order but does not, dismissal is not an abuse of discretion even where willfulness or bad faith is not shown); Merritt v. Int'l Bhd. of Boilermakers, 649 F.2d 1013, 1019 (5th Cir. 1981) (finding that bad faith not required for imposing sanction of reasonable expenses and attorney's fees in connection with a motion to compel discovery); cf. Law Enforcement Alliance of Am., Inc. v. USA Direct, Inc., No. 02-1715, 2003 WL 1154115, at *7 (4th Cir. Mar. 14, 2003) (holding that bad faith is one factor in a four factor test in applying Rule 37 sanctions: "Where a district court determines that there was no bad faith, that determination will likely by reflected in a less severe sanction [than dismissal]. Anderson [v. Found. for Advancement, Educ. and Employment of Am. Indians, 155 F.3d 500, 504 (4th Cir. 1998)] does not require a finding of bad faith before discovery sanctions can be awarded and to hold otherwise would be at odds with Rule 37(c)(1)'s plain language, which contains no such requirement."); Poulis v. State Farm Fire and Cas. Co., 747 F.2d 863, 867-68 (3d Cir. 1984) (listing "whether the conduct of the party of the attorney was willful or in bad faith" as one of six factors to be weighed by a court considering a sanction of dismissal under Rule 37; no one factor is determinative). See also Tennant Co. v. Hako Minuteman, Inc., 878 F.2d 1413, 1416 (Fed. Cir. 1989) (noting that when interpreting Rule 37, Federal Circuit applies the law of the regional circuit to which the district court appeals normally lie).

[FN47]. See Stevenson, 354 F.3d at 748 (affirming adverse inference instruction where destroyed voice tape was "the only recording of conversations between the engineer and dispatch contemporaneous with the accident render[ing] its loss prejudicial to the plaintiffs"); Zubulake v. UBS Warburg, LLC, No. 02 Civ. 1243, 2004 WL 1620866 (S.D.N.Y. July 20, 2004) (giving adverse inference instruction because plaintiff prejudiced by spoliation of electronic documents); Mosaid Techs. Inc. v. Samsung Elecs. Co., No. 01 CV 4340, 2004 U.S. Dist. LEXIS 23596, at *7 (D.N.J. July 7, 2004) (granting adverse inference instruction in case where "[t]he prejudice resulting from complete and total email spoliation seems particularly obvious"); In re Heritage Bond Litig., 223 F.R.D. 527 (C.D. Cal. 2004) (precluding defendants from defending against allegations that they fraudulently transferred the marital residence because failure to produce Quicken files prejudiced the plaintiffs by preventing them from preparing their case); Thompson v. United States Dep't of Hous. and Urban Dev., 219 F.R.D. 93 (D. Md. 2003) (discussed in text); DeLoach v. Philip Morris Co., 206 F.R.D. 568 (M.D.N.C. 2002) (permitting plaintiffs to respond to defendant's expert rebuttal report but not permitting defendants to reply, since information provided to defendant's expert was not made available to plaintiffs until after plaintiff's expert could no longer make use of it); Trigon Ins. Co. v. United States, 204 F.R.D. 277 (E.D.Va. 2001) (adverse inference instruction appropriate because plaintiff had suffered prejudice in the form of a diminished ability to cross-examine the testifying experts); Sheppard v. River Valley Fitness One, L.P., 203 F.R.D. 56, 60 (D.N.H. 2001) (precluding witness from testifying about settlement because defendant failed to produce computer records before depositions, which "unfairly prejudiced the plaintiffs by depriving them of the opportunity to question [the witness] about the contents of the documents"). But see W.R. Grace & Co.-Conn. v. Zotos Int'l, Inc., No. 98-CV-838S, 2000 WL 1843258 (W.D.N.Y. Nov. 2, 2000) (awarding expenses incurred in connection with the sanctions motion, but reserving judgment on further sanction pending discovery regarding whether documents could be reconstructed and the degree of resultant prejudice).

[FN48]. 219 F.R.D. 93 (D. Md. 2003).

[FN49]. Id. at 101.

[FN50]. Id. at 103.

[FN51]. Id. at 103 n.9.

11 MITTLR 71
11 Mich. Telecomm. & Tech. L. Rev. 71
(Cite as: 11 Mich. Telecomm. & Tech. L. Rev. 71)

[FN52]. Id. at 104-05.

[FN53]. Id. at 105.

[FN54]. Id.

[FN55]. See 745 N.Y.S.2d 70 (N.Y. Ct. App. 2002) (affirming trial court's dismissal).

[FN56]. See YCA, LLC v. Berry, No. 03 C 3116, 2004 WL 1093385 (N.D. Ill. May 7, 2004) (finding the delay in production justified and that there was no prejudice); Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162 (S.D.N.Y. 2004) (noting that plaintiff only established that witnesses communicated by email from time to time, but had not made an effort to determine the substance of those communications in any but the most general terms); Wiginton v. Ellis, No. 02 C 6832, 2003 WL 22439865 (N.D. Ill. Oct. 27, 2003) (if back up tapes showed that relevant documents had been destroyed, then plaintiff should renew motion for appropriate sanctions based on the destroyed evidence); Williams v. Saint-Gobain Corp., No. 00-CV-0502E, 2002 WL 1477618 (W.D.N.Y. June 28, 2002) (extending discovery because the violation could be corrected); Hildreth Mfg., LLC v. Semco, Inc., 785 N.E.2d 774, 782 (Ohio Ct. App. 2003) (finding "no reasonable possibility that the missing hard drives contained evidence of the theft of trade secrets" because the erased hard drives were installed after issuance of a temporary restraining order, with defendant "fully aware that these computers were subject to discovery"); Eichman v. McKeon, 824 A.2d 305 (Pa. Super. 2003) (noting that plaintiffs were able to, and did, cross-examine the defense experts regarding their opinions, and although plaintiffs were given opportunity to present rebuttal evidence regarding computer logs and the loss of the claim file, they chose not to do so).

[FN57]. 2004 WL 1093385, at *5.

[FN58]. Id.

[FN59]. Id.

[FN60]. Id. at *7.

[FN61]. Id.

[FN62]. See Inst. for Motivational Living, Inc. v. Doulos Inst. for Strategic Consulting, Inc., No. 03-4177, 2004 WL 2241745 (3d Cir. Oct. 5, 2004) (granting attorney's fees and costs where defendant deleted files from laptop computer the morning he turned it over to plaintiff); Minn. Mining & Mfg. v. Pribyl, 259 F.3d 587 (7th Cir. 2001) (imposing adverse inference instruction where defendant wiped his hard drive by downloading six gigabytes of music the night before he was to hand over his computer); Advantacare Health Partners v. Access IV, No. C 03-04496, 2004 WL 1837997 (N.D. Cal. Aug. 17, 2004) (instructing trier of fact to find that defendants had copied all of the files on plaintiff's computer as sanction for using software deletion program to cover up illegal copying of files from plaintiff); Invision Media Communications, Inc. v. Fed. Ins. Co., No. 02 Civ. 5461, 2004 WL 396037 (S.D.N.Y. Mar. 2, 2004) (awarding attorney's fees and costs to defendant because plaintiff made false representations about the existence and location of relevant documents in conscious and bad faith effort to hinder insurance company's investigation); Anderson v. Crossroads Capital Partners, LLC, No. Civ. 01-2000, 2004 WL 256512 (D. Minn. Feb. 10, 2004) (giving adverse inference instruction because plaintiff willfully deleted computer files using data wiping program); In re Heritage Bond Litig., 223 F.R.D. 527 (C.D. Cal. 2004) (precluding defendants from defending against a claim because they willfully failed to comply with the court's order); Network Computing Servs. Corp. v. Cisco Sys., Inc., 223 F.R.D. 392 (D.S.C. 2004) (allowing defendant to inform jury of plaintiff's discovery misconduct); Kucala Enters., Ltd. v. Auto Wax Co., Inc., No. 02 C 1403, 2003 WL 22433095 (N.D. Ill. May 27, 2003) (permitting jury to hear evidence of plaintiff's destruction of computer evidence with Evidence Eliminator software program, for purpose of determining damages and willfulness issues); Cobell v. Norton, 206 F.R.D. 324 (D.D.C. 2002) (sanctioning defendant for moving for protective order clarifying its duty to produce email because the issued had been raised three times before); Pennar Software Corp. v. Fortune 500 Sys. Ltd., No. 01-01734, 2001 U.S. Dist. LEXIS 18432 (N.D. Cal. Oct. 25, 2001) (awarding attorney's fees and costs because defendants deleted web pages that plaintiffs wanted to use to establish personal jurisdiction over defendants); Lombardo v. Broadway Stores, Inc., No. G026581, 2002 WL 86810 (Cal. Ct. App. Jan. 22, 2002) (ordering defendant to pay plaintiff's attorney's fees because willfully destroyed computer files); Bandy v. Cincinnati, New Orleans and Tex. Pac. Ry. Co., No. 2001-CA-002121, 2003 WL 22319202 (Ky. Ct. App. Oct. 10, 2003) (giving adverse inference instruction in response to deliberate and intentional failure to cooperate in discovery process); Munshani v. Signal Lake Venture Fund II, 805 N.E.2d 998 (Mass. App. Ct. Mar. 26, 2004) (dismissing plaintiff's complaint because plaintiff committed fraud on the court by fabricating e-mail evidence); Comm'r of Labor v. Ward, 580 S.E.2d 432 (N.C. Ct. App. 2003) (striking defendants' answer and default judgment on certain claims because defendants failed to provide plaintiffs with electronically stored information in repeated violation of the court's discovery order and in the face of explicit warnings that sanctions would be imposed); QZO, Inc. v. Moyer, 594 S.E.2d 541 (S.C. Ct. App. 2004) (entering default judgment where defendant reformatted hard drive before producing it to plaintiff).

[FN63]. See Computer Task Group, Inc. v. Brotby, 364 F.3d 1112 (9th Cir. 2004) (entering default judgment where defendant engaged in systematic discovery abuse, including refusal to produce documents and making incredible excuses, such as earthquake and dropped computer, for non-production); Metropolitan Opera Ass'n. v. Local 100, 212 F.R.D. 178 (S.D.N.Y. 2003) (entering default judgment against defendants to deter similar conduct by others, remedy the effect of the discovery abuses, and punish the parties responsible for spoliation); Mariner Health Care, Inc. v. PriceWaterhouseCoopers LLP, No. 02VS037631-F, slip op. (Ga. Fulton Cty. Nov. 9, 2004) (dismissing complaint with prejudice because lesser sanctions would have been ineffective in changing plaintiff's bad faith behavior); Munshani, 805 N.E.2d 998 (dismissing complaint was one of the few ways to deter fraud on the court); Ward, 580 S.E.2d 432 (entering default judgment on some claims because defendants failed to provide plaintiffs with copies of electronic data and failed to answer deposition questions regarding the method of access to information stored on the tapes); Essex Group v. Express Wire Servs., 578 S.E.2d 705 (N.C. Ct. App. 2003) (imposing default judgment in order to prevent or eliminate defendant's dilatory and dishonest tactics).

[FN64]. See Metropolitan Opera, 212 F.R.D. at 229 (noting that plaintiff had been prejudiced by defendants' discovery failures because it was denied the opportunity to plan its strategy in an organized fashion as the case proceeded); Mariner, No. 02VS037631-F, slip op. (finding that defendant had been prejudiced in their preparation for depositions).

[FN65]. No. 02VS037631-F, slip op.

[FN66]. Id. at 57-64.

[FN67]. Id. at 57-58.

[FN68]. Id. at 26.

[FN69]. Id.

[FN70]. Id. at 26-27.

[FN71]. Id. at 2.

[FN72]. For example, after the court granted Mariner's request the production deadline, it missed the deadline and waited until the month before the start of depositions to begin delivering over 25% of the total documents, most of which related to central issues in the case. See id. at 36.

[FN73]. Id. at 57.

[FN74]. Id. at 34-35, 37.

[FN75]. Id. at 4.

[FN76]. Id. at 5.

[FN77]. Id. at 66.

[FN78]. Id. at 67.

11 MITTLR 71
11 Mich. Telecomm. & Tech. L. Rev. 71
(Cite as: 11 Mich. Telecomm. & Tech. L. Rev. 71)

© 2006 Thomson/West. No Claim to Orig. U.S. Govt. Works.

[FN79]. Id. at 66-67.

[FN80]. See No. 5:98-cv-2876, slip op. at 72 (N.D. Ohio July 16, 2004).

[FN81]. See id. at 67.

[FN82]. See id.

[FN83]. See id.

[FN84]. Id. at 67-68.

[FN85]. See id. at 49-50.

[FN86]. Id. at 71-72.

[FN87]. See supra notes 62-64.

[FN88]. See Morris v. Union Pac. R.R. Co., 373 F.3d 896 (8th Cir. 2004) (adverse inference instruction should not have been given where there was an absence of information to support an inference of conscious destruction of tape); Williams v. Ehlenz, No. Civ. 02-978, 2004 WL 742076 (D. Minn. Mar. 30, 2004) (noting that tapes had been destroyed in accordance with prison policy before magistrate judge had ordered that they be produced); Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162 (S.D.N.Y. 2004) (noting that there was no evidence of intentional destruction); Williams v. Saint-Gobain Corp., No. 00-CV-0502E, 2002 WL 1477618 (W.D.N.Y. June 28, 2002) (denying sanction because defendant produced e-mails as soon as it had received them, "albeit on the eve of trial--and there is no evidence of any bad faith as to any withholding or destruction of the same"); Tomlin v. Wal-Mart Stores, Inc., 100 S.W.3d 57, 64-65 (Ark. Ct. App. Mar. 12, 2003) (finding no indication that the missing strapping band that caused the slip and fall was "bad" evidence); United States v. Murphy Oil USA, Inc., 155 F. Supp. 2d 1117 (W.D. Wis. 2001) (finding nothing in the record to indicate bad faith by the employees or that the evidence would have been favorable to defendants); Eichman v. McKeon, 824 A.2d 305 (Pa. Super. 2003) (finding that there had been no willful discovery violation); Crescendo Invs., Inc. v. Brice, 61 S.W.3d 465 (Tex. App. 2001) (refusing to grant spoliation instruction because affidavit established that shareholder did not act with fraudulent intent in destroying weekly and biweekly e-mail reports); Yao v. Bd. of Regents of Univ. of Wis. Sys., 649 N.W.2d 356 (Wis. Ct. App. 2002) (surveillance tapes deleted at a time when it was not apparent that they would be significant and were not destroyed in order to impede the case).

[FN89]. In approximate order of declining prejudice: See Thompson v. United States Dep't of Hous. and Urban Dev., 219 F.R.D. 93 (D. Md. 2003), 219 F.R.D. 93 (prejudice); Sheppard v. River Valley Fitness One, L.P., 203 F.R.D. 56 (D.N.H. 2001) (prejudice); Playball at Hauppauge, Inc. v. Narotzky, 745 N.Y.S.2d 70 (N.Y. Ct. App. 2002) (prejudice); DeLoach v. Philip Morris Co., 206 F.R.D. 568 (M.D.N.C. 2002) (prejudice); Wadja v. Kingsbury, 652 N.W.2d 856 (Minn. Ct. App. 2002) (prejudice); Mosaid Techs. Inc. v. Samsung Elecs. Co., No. 01 CV 4340, 2004 U.S. Dist. LEXIS 23596 (D.N.J. July 7, 2004) (prejudice, recklessness); Trigon Ins. Co. v. United States, 204 F.R.D. 277 (E.D.Va. 2001) (finding of willfulness, but emphasis on prejudice); In re Heritage Bond Litig., 223 F.R.D. 527 (C.D. Cal. 2004) (prejudice, willfulness); Zubulake v. UBS Warburg, LLC, No. 02 Civ. 1243, 2004 WL 1620866 (S.D.N.Y. July 20, 2004) (prejudice, willfulness); Thomas v. Isle of Capri Casino, 781 So.2d 125 (Miss. 2001) (prejudice, gross negligence); MasterCard Int'l, Inc. v. Moulton, No. 03 Civ. 3613, 2004 WL 1393992 (S.D.N.Y. June 22, 2004) (prejudice, gross negligence); Stevenson v. Union Pac. R.R. Co., 354 F.3d 739 (8th Cir. 2004) (prejudice, bad faith); Advantacare Health Partners v. Access IV, No. C 03-04496, 2004 WL 1837997 (N.D. Cal. Aug. 17, 2004) (prejudice, willfulness and bad faith); United States v. Philip Morris USA, Inc., 327 F. Supp. 2d 21 (D.D.C. 2004) (finding of prejudice, but emphasis on reckless disregard and gross indifference); Computer Task Group, Inc. v. Brotby, 364 F.3d 1112 (9th Cir. 2004) (willfulness, prejudice); Metropolitan Opera Ass'n. v. Local 100, 212 F.R.D. 178 (S.D.N.Y. 2003) (prejudice, high willfulness and bad faith); Mariner, No. 02VS037631-F, slip op. (prejudice, high willfulness and bad faith); Anderson v. Crossroads Capital Partners, LLC, No. Civ. 01-2000, 2004 WL 256512 (D. Minn. Feb. 10, 2004) (willfulness); Montage Group, Ltd. v. Athle- Tech Computer Sys., Inc., No. 2D03-2026, 2004 WL 2892394 (Fla. Ct. App. Oct. 13, 2004) (willfulness); Kucala Enters., Ltd. v. Auto Wax Co., Inc., No. 02 C 1403, 2003 WL 22433095 (N.D. Ill. May 27, 2003) (willfulness); Network Computing Servs. Corp. v. Cisco Sys., Inc., 223 F.R.D. 392 (D.S.C. 2004) (willfulness); Pennar Software Corp. v. Fortune 500 Sys. Ltd., No. 01-01734, 2001 U.S. Dist. LEXIS 18432

(N.D. Cal. Oct. 25, 2001) (willfulness, bad faith); Inst. for Motivational Living, Inc. v. Doulos Inst. for Strategic Consulting, Inc., No. 03-4177, 2004 WL 2241745 (3d Cir. Oct. 5, 2004) (willfulness, bad faith).

[FN90]. No. 01 CV 4340, 2004 U.S. Dist. LEXIS 23596 (D.N.J. July 7, 2004).

[FN91]. 327 F. Supp. 2d 21 (D.D.C. 2004).

[FN92]. 212 F.R.D. 178 (S.D.N.Y. 2003).

[FN93]. 2004 U.S. Dist. LEXIS 23596, at *7-8.

[FN94]. Id. at *7.

[FN95]. Id. at *7-8.

[FN96]. Id. at *7.

[FN97]. Id.

[FN98]. Id.

[FN99]. Mosaid Techs. Inc. v. Samsung Elecs. Co., 224 F.R.D. 595, 599 (D.N.J. Sept. 1, 2004).

[FN100]. Id. at 600.

[FN101]. Id.

[FN102]. Id. (citing Zubulake v. UBS Warburg, LLC, No. 02 Civ. 1243, 2004 WL 1620866 (S.D.N.Y. July 20, 2004)).

[FN103]. Id.

[FN104]. Mosaid Techs. Inc. v. Samsung Elecs. Co., No. 01 Civ. 4340, 2004 U.S. Dist. LEXIS 25286, at *21 (D.N.J. Dec. 7, 2004).

[FN105]. See Mosaid, 2004 U.S. Dist. LEXIS 25286.

[FN106]. Id. at *15-16.

[FN107]. 327 F. Supp. 2d 21, 26 (D.D.C. 2004).

[FN108]. Id. at 23.

[FN109]. Id. at 23-24.

[FN110]. Id. at 25.

[FN111]. Id. This case is being conducted as a bench trial. As noted by the Thompson court, an adverse inference instruction does little, if anything, in a bench trial because a judge is able to draw reasonable inferences from the defendants' spoliation. See 219 F.R.D. at 105.

[FN112]. Philip Morris, 327 F. Supp. 2d at 25.

[FN113]. Id. at 26.

[FN114]. Id.

11 MITTLR 71
11 Mich. Telecomm. & Tech. L. Rev. 71
(Cite as: 11 Mich. Telecomm. & Tech. L. Rev. 71)

[FN115]. 212 F.R.D. 178 (S.D.N.Y. 2003).

[FN116]. Id. at 224.

[FN117]. Id. at 221.

[FN118]. Id. at 222-29.

[FN119]. Id. at 182.

[FN120]. Id. at 224.

[FN121]. Id. at 230.

[FN122]. See 2004 WL 1943099 (S.D.N.Y. Aug. 27, 2004).

[FN123]. Electronic information had been lost in 84% of the cases granting sanctions, and 87% of the cases denying sanctions.

[FN124]. See supra note 89 and accompanying text.

END OF DOCUMENT