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

SECOND EDITION
NOVEMBER 2007

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

2007 Editor in Chief:
Lori Ann Wagner

2005 Editors in Chief:
Charles R. Ragan
Jonathan M. Redgrave
Lori Ann Wagner

2005 Senior Editors:
Christine M. Burns
David Kittrell
Judy Van Dusen

2005 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℠

Copyright © 2007
The Sedona Conference®
Visit www.thesedonaconference.org

Foreword

Welcome to *THE SEDONA GUIDELINES: Best Practice Guidelines & Commentary for Managing Information & Records in The Electronic Age (2nd Edition) ("The Sedona Guidelines")*, 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 ("WGS 1") was electronic document production in the context of litigation. That effort resulted in *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery* (2005) (originally published in 2003 for public comment), which was revised and re-published in June of 2007 as *The Sedona Principles, Second Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery*.

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 WGS 1 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, in its original form, was published for a six month public comment period on September 1, 2004, and following substantial re-writing, presentation and discussion at various forums, a final version was published in September 2005. Additional case law developments, and the adoption of the amendments to the Federal Rules of Civil Procedure related to electronically stored information, caused the editorial board to re-visit the 2005 publication, and the result here is an updated look at information and records management in the electronic world.

The Working Group in the future will continue to publish "commentaries" and other work product targeting specific issues and developments in the area of information and records management. Details of these activities are regularly 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; but may find it useful to do so in some instances.

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 often are 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 of the 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 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]

---

[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] In 2004, the U. S. National Archives and Records Administration (NARA) announced the award of a contract to Lockheed Martin Corporation for the agency's new Electronic Records Archive (ERA), which was launched as a project in 1998. http://www.archives.gov/era/about/index.html#background. The goals for the system are to "capture electronic information, regardless of its format, save it permanently, and make it accessible on whatever hardware or software is currently in use." http://www.archives.gov/press/press-releases/2004/nr04-73.html. While a functional subset of the ERA is expected to become operational sometime in 2008, full implementation will take years and, even if it proves successful, only answers the question of "how" to store electronic records and not "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."

[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 F. A description of The Sedona Conference® and its Working Group Series is set forth in Appendix G.

Table of Contents

Introduction

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

The "computer revolution" has brought about momentous change over the past twenty years in the way society creates, communicates and stores information. Yet, laws and policies have been very slow to adapt to this new paradigm involving immense volumes, high volatility and great mobility of electronic information. Moreover, lacking 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.[5]

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.[6]

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. Instead, they are intended to provide guidance to organizations in determining a course of action throughout the challenging process of managing electronic information and records.

2. "Managing"[7] Information and Records

From a traditional records management perspective[8] information should be retained as long as it has value to an

---

[5] *See, e.g.*, *2005 Electronic Records Management Survey - A Renewed Call to Action*, Cohasset Associates, Inc. available for download at http://www.merresource.com/downloadWhitepaper.htm?fileId=1 and *2007 Electronic Records Management Survey – A Call for Collaboration*, Cohasset Associates, Inc., available for download at ; *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 9/27/2007).

[6] 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).

[7] 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.

[8] 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.

organization, or is required by law or regulation to be retained.[9] 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[10] and in some cases *must* be destroyed.[11]

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."[12] 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. 696, 125 S. Ct. 2129, 2135 (2005).[13]

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 "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.

---

[9] 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).

[10] 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.

[11] 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, in its 2005 complaint against BJ's Wholesale Club, the FTC raised the issue of what constitutes an appropriate retention period for personal information. In its complaint the FTC alleged BJ's "created unnecessary risks to the [personal customer] information by storing it for up to 30 days when it no longer had a business need to keep the information…" (*In the matter of BJ's Wholesale Club, Inc.,* FTC Docket No. C-4148, 2005). Additionally, 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).

[12] *Arthur Andersen, LLP v. United States*, 544 U.S. 696, 125 S. Ct. 2129, 2135 (2005). Importantly, it must be noted that the Supreme Court's decision did *not* endorse the actions or *Arthur Andersen, LLP v. United States*, 544 U.S. 696, 125 S. Ct. 2129, 2135 (2005). 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.

[13] 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).

"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.[14] 44 U.S.C. § 3301 (2000). 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.

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 was estimated that eighty-five percent (85%) of corporate data resides in unstructured formats outside of databases.[15]

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

Appropriate management of information and records is driven by two primary sources: (a) statutory, regulatory and other legal principles ("the law"), and (b) professional standards.

---

[14] 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.

[15] Eric Auchard, "Search concepts, not keywords, IBM tells business" (Reuters Aug. 8, 2005), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/08/08/AR2005080800004.html.

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. Most statutes and regulations encompass both electronic and traditional paper records in their definitions of "document" or "record," the exception being state security breach notification laws, many of which reference only electronically stored data. 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).

In addition, the common law creates obligations to preserve *evidence* (whether designated as records or not) when actual or reasonably anticipated litigation is involved.

Professional Standards: Many trade and service organizations recommend that their members follow published standards and technical papers addressing records and information management issues. Furthermore, within certain industries, trade practices regarding data capture and retention may become standards for all industry members. 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). 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 are accredited international standards development organizations that issue standards and reports regarding records and information management.

In 2001, ISO sought an international consensus standard for records management, including electronic records, in its guidance document ISO Technical Report 15489-2 (*Information and Documentation—Records Management* (2001)) and its accompanying standard, ISO 15489-1.[16] 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.[17]

The organizations mentioned above 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 (and increasingly in other countries as "American-style" litigation practices are exported overseas), that we address in Guideline 5 and its accompanying text.

---

[16] 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.

[17] 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).

Apart from the standards and guidelines offered by standards and trade organizations,[18] many consultants, vendors and software companies offer solutions to the complex questions involved in managing information and records in the electronic age. Some even provide white papers and technical reports to assist organizations researching solutions in the area (often free-of-charge as downloads from their website). However, it is important to read such information with a critical eye towards determining whether the recommendations advocate a narrow approach to information management tied to the solutions offered by the vendor/author and will be practical in the particular organization.

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, 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 identification of and 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;
- Facilitating statutory notification requirements in the event of a security breach involving personal information;
- 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 the 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 much 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.

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:

---

[18] 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.

- 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;
- Failure to comply with security breach notification 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;[19]
- Civil litigation consequences, such as increased litigation costs, fines,[20] adverse inference instructions,[21] default judgment,[22] and civil contempt;[23]
- Vicarious liability for responsible senior management;[24] and
- Criminal liability for organizations[25] and individuals.[26]

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.

---

[19] *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.

[20] *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).

[21] *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*, 229 F.R.D. 442 (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).

[22] *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).

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

[24] 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).

[25] 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. 596, 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. § 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. 596, 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.

[26] A significant 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:

7. Enormous Challenges and Reasonable Expectations: the Road Ahead

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

Footnote 26 cont.

- 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.

The SEC and the Public Company Accounting Oversight Board (PCAOB) held public meetings in 2005 and 2006 to solicit feedback on companies' experiences in complying with the Act. See "PCAOB Documents" available at http://www.sec.gov/spotlight/soxcomp.htm (visited August 21, 2008). Complaints about the high costs of compliance, particularly for smaller organizations, resulted in various proposals to reform the internal financial controls section of the Act. A proposal to amend the Act to make compliance with Sarbanes-Oxley's Section 404 optional for companies with total market value of less than $70 million was rejected by the Senate in April 2007. However, additional reform proposals are still under consideration. *See, e.g.,* H.R. 1508 (introduced March 13, 2007) and S. 869 (introduced March 14, 2007) ("A bill to reform certain provisions of section 404 of the Sarbanes-Oxley Act of 2002, to make compliance with that section more efficient, with the goal of maintaining United States capital market global competitiveness.").

- 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."[23] 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).

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.

The Sedona Guidelines for Managing Information and 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 retain metadata, however they may wish to do so in some instances.

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)). 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 faced stiff fines and damage to their reputation when consumer records laden with sensitive private information have been breached or inexplicably "lost," triggering costly notification and (in some states) credit monitoring services under state security breach laws.

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, chief compliance 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 on 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.

Organizations are also well served by examining and inventorying their various sources and locations of electronic documents and information in light of the 2006 amendments to the Federal Rules of Civil procedure relating to electronically stored information ("ESI"). Organizations need to have sufficient knowledge about their information systems to impose an appropriate legal hold and meet their obligations to preserve, disclose, collect and produce potentially relevant ESI. Outside counsel may be well advised to encourage reliable inventories. In one case the court found monetary sanctions appropriate when counsel relied solely on the client's statements about the location of

relevant data, finding counsel failed to conduct an adequate investigation and had a duty to inquire about sources of information. *See Phoenix Four v. Strategic Res. Corp.*, 2006 WL 1409413 (S.D.N.Y. May 23, 2006). An exemplar "survey of data" containing potential inquiries for self-examination is included as Appendix C.

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. 696, 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.,* 229 F.R.D. 506 (D. Md. 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; *see also Bass-Davis v. Davis,* 134 P.3d 103, 110 (Nev. 2006) ("[W]illful suppression or destruction . . . requires more than simple destruction of evidence and instead requires that evidence be destroyed with the intent to harm another party."), *overruling in part Reingold v. Wet 'N Wild Nev., Inc.* 944 P.2d 800, 802 (Nev. 1997) (adverse inference instruction appropriate where party's document retention policy resulted in destruction of documents prior to expiration of statute of limitations on potential claims).

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. 696, 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."); *Hynix Semiconductor Inc. v. Rambus, Inc.,* 2006 WL 565893 (N.D. Cal. Jan. 5, 2006) (adoption of a "content-neutral" document retention and destruction policy is a "permissible business decision")[27] ; 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."); *see also Consol. Aluminum Corp. v. Alcoa, Inc.,* 2006 WL 2583308 (M.D. La. July 19, 2006) (quoting *Zubulake*); *Durst v. FedEx Express,* 2006 WL 1541027 at *5 (D. N.J. June 2, 2006) ("A litigant 'is under no duty to keep or retain every document in its possession ... [only] what it knows, or reasonably should know, will likely be requested in reasonably foreseeable litigation.'") (citing *Costello v. City of Brigatine,* 2001 U.S. Dist. LEXIS 8687 at *75 (D.N.J.2001); *Computek Computer & Office Supplies, Inc. v. Walton,* 156 S.W.3d 217 (Tex. App. 2005) (finding injunction prohibiting plaintiff from removing or deleting any files in its possession overbroad; court held that plaintiff had a legal right to delete its own records and files unrelated to the 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, 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, unreasonable and ineffective.

[27] See further discussion of *Rambus* case and related litigation in discussion of Comment 2.c, below.

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 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.

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 information and records management policies and procedures are numerous and complex. Among the variables to be considered, which are discussed in these Guidelines, are:

- 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.);[28]
- 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, destruction and security requirements (*e.g.*, through published retention schedules or through means embedded within software applications or in business procedures or some combination thereof);

[28] 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.

- 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.

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.

From a records management perspective, appropriately managed information is retained only so long as it has value to an organization or is required by law or regulation to be retained. Typically, these retention periods are reflected in an organization's records retention schedule. Reliance on the schedule pre-supposes that the appropriate decisions have been made concerning the length of time something has value and whether its retention is subject to a legal or regulatory obligation.[29]

The true measure of a good records and information management policy is whether it allows the organization to meet its legal and regulatory obligations, and meet whatever internal goals the organization has set for the policy (*e.g.,* reduce the cost of storage by reducing the amount of information that is stored; reduce the time involved in retrieving valuable information; protect information that supports intellectual property rights). However, these are generally intangible matters and it is usually in the context of litigation (or government investigation such as the *Arthur Andersen* case) that such programs are judged.

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, FTC, state and federal privacy laws and regulations, 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)[30] ; *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 was documented in a records retention schedule.[31] Today, in light of the tremendous volumes of information being generated and received and the decentralized management of the content of electronically stored information (*i.e.*, individual users are often the content owners), it is becoming increasingly important for organizations to consider consolidating their

[29] Importantly, it is the schedule which should control retention, rather than an independent ("in-the-moment") decision by each employee as to value. While an individual employee may be required to determine whether a specific piece of information (*e.g.* an e-mail, a hard copy memorandum or letter, or an instant message) fits within a records type, he or she is not determining the inherent value of the information and how long it should be kept based on that assessment.

[30] See further discussion of the *Rambus* litigations, including a court which reached the opposite conclusion, below.

[31] 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, even despite incorporation of language in the organization's policies purporting to cover electronic records.

retention schedules. Thus, some organizations are turning to "bucketed" approaches that dramatically limit the number of mandatory classifications that must be made by individuals, while ensuring that the minimum retention periods for information are met.

Regardless of nomenclature, an organization's overall strategic thinking about managing information should be the same for electronic records as for paper records, as it is the content rather than the format that matters (*i.e.*, the retention schedule is generally media neutral).[32] Importantly, with the enactment of 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 § 216 of FACTA and requiring proper disposal of consumer information so as to protect against unauthorized access).

Beyond the strict legal requirements,[33] a reasonable policy can serve the legitimate information storage, access, security and retention needs of the organization.[34] 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).[35] 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 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.

---

[32] 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.

[33] 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.

[34] 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.

[35] 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).

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 internally discussing 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. *Rambus v. Infineon* was tried to the court in February 2005. At the close of the evidence, the court found by clear and convincing evidence that the plaintiff had "unclean hands" due to its spoliation of evidence, barring it from enforcing the patents in suit and that dismissal was appropriate. Before the court could issue findings and conclusions, the parties settled the case.

The question of whether Rambus implemented and followed in good faith a reasonable records retention policy and/or reasonably anticipated litigation when it destroyed documents pursuant to that policy has been the subject of numerous other actions. In *Hynix Semiconductor, Inc. v. Rambus, Inc.*, 2006 WL 565893 (N.D. Cal. Jan. 5, 2006), the Northern District of California reached the opposite conclusion reached by the court in the Eastern District of Virginia. Holding that because the path to the initiation of litigation was neither "clear nor immediate" and because numerous conditions needed to be met first, the court found it could not conclude that Rambus anticipated litigation and that the evidence did not support the conclusion that Rambus intentionally designed its document retention policy to get rid of damaging documents. *Id.* at *21-*25. However, the Eastern District of Virginia was not swayed from its position when in July 2006 it issued another opinion finding that Rambus had engaged in spoliation of evidence, but refusing to award attorneys' fees to Samsung because it did not prove that the attorneys' fees sought were related to the misconduct. *See Samsung Electronics Co., LTD v. Rambus, Inc.*, 2006 WL 2038417 (July 18, 2006 E.D.Va.)

Finally, while the FTC held that it did not need to resolve whether Rambus engaged in spoliation because it had already found Rambus guilty on the merits, it stressed that:

> Rambus' extensive document destruction campaign had the potential to deny the Commission an opportunity to examine thoroughly Rambus' conduct. In some instances, the Commission relied on evidence that was preserved only fortuitously. If the record in this case had been marginal, while simultaneously containing evidence that Rambus destroyed potentially relevant documents, we would have pursued the spoliation inquiry to its conclusion and, if appropriate, imposed a remedy.

See Opinion of the Commission, In the Matter of Rambus, Inc., Docket No. 9302 (August 2, 2006). *See also Kozlowski v. Sears, Roebuck & Co.*, 73 F.R.D. 73, 76 (D. Mass. 1976) (a party cannot excuse itself from compliance with discovery rules by adopting a records management system designed to make discovery unduly difficult). *Compare Arthur Andersen, LLP v. United States*, 544 U.S. 696, 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. § 1512(b)(2) ; *Bass-Davis v. Davis*, 134 P.3d 103, 110 (Nev. 2006). (evidence destroyed as part of a document retention policy before any notice of an obligation to retain that evidence is not willful suppression, absent any evidence that the destruction was done to harm another party), *overruling in part 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").

> ***Illustration ii.*** Acme Corporation's stock prices have been dropping and current management 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.[36] *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 six years 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.

[36] Appendix C 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 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.

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.[37] 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 amendments to the Federal Rules of Civil Procedure 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* Fed. R. Civ. P. 26 (as amended December 1, 2006)[38] . 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.

---

[37] *Cf.* Marianne Swanson *et al.*, *National Institute of Standards and Technology, Contingency Planning Guide for Information Technology Systems* (Dep't of Commerce 2002).

[38] The 2006 amendments to the Federal Rules of Civil Procedure addressing the discovery of electronically stored information became effective December 1, 2006. See http://www.uscourts.gov/rules.gov/rules/EDiscovery_w_Notes.pdf. The amendments impact rules 16, 26, 33, 34, 37, 45 and Form 35. Unless otherwise indicated, all references to the Federal Rules of Civil Procedure and accompanying Committee Notes are to the language in force December 1, 2006. Shortly after completion of the amendments addressing electronic discovery, the entire Federal Rules of Civil Procedure underwent "restyling," a process intended to clarify and simplify the language and presentation of the rules without affecting their substantive meaning. See http://www.uscourts.gov/rules/supct1106/CV_CLEAN_FINAL5-30-07.pdf. The restyled rules are anticipated to go into effect December 1, 2007.

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;"[39]
- What will be stored for access in the event of a "disaster;"
- Who has responsibility for duplicating and managing electronic information;
- 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. Retention of disaster recovery backup media beyond the period necessary to recover from a true disaster can have unintended consequences should the organization become involved in litigation. In *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc., No. 502003CA005045XXOCAI, 2005 WL 679071 (Fla Cir. Ct. Mar. 1, 2005), further opinion 2005 WL 674885 (Mar. 23, 2005), rev'd and remanded on other grounds, —-So.2d ——, 2007 WL 837221 (Fla. Dist. Ct. App. Mar. 21, 2007)*, Morgan Stanley's continual locating of additional backup tapes despite certifications that all potentially relevant information had been located and searched derailed the substance of the litigation. Concluding that defendant had sought to thwart discovery, and had failed through "willful and gross abuse", "grossly negligent and negligent conduct" with respect to discovery obligations to timely locate and produce relevant information from more than 1,000 backup tapes, the court reversed the burden of proof and instructed the jury that Morgan Stanley had to prove that it did not defraud the plaintiff. The jury returned verdicts of $605 million in compensatory damages and $850 million in punitive damages.[40]

> ***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, having read that "storage is cheap" and thinking that the cost is the incremental cost for additional storage tapes. Unknown to the VP, 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

---

[39] *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).

[40] In a split opinion the Florida District Court of Appeal reversed the verdict and remanded the case to the lower court with directions to enter judgment for Morgan Stanley based the failure of the plaintiff to offer proof of its compensatory damages at trial. Because in its view this issue was dispositive of the case as to both compensatory and punitive damages, the majority opinion did not address the e-discovery issues. The dissent, which would have affirmed the verdict on compensatory damages, but remanded the punitive damages verdict for further proceedings, obliquely raised the issue of e-discovery. In footnote 4 the dissenting opinion states: "I agree that the trial court did not abuse its discretion in the sanctions imposed on Morgan Stanley for substantial violations of court orders."

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.

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

Comment 3.a.
Destruction[41] 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. 696, 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, Second Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery (The Sedona Conference® Working Group Series, 2007)* ("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.").[42]

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.[43]

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 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."). *See also, "Hit 'Delete' to Prevent EDD Disaster"*, Stanley M. Gibson (August 7, 2007) at http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1186412327538&pos=ataglance (last accessed 9/27/2007). An organization can control these

---

[41] We use the word "destruction" so there is no ambiguity. An organization, in drafting its policy, may use different terminology.

[42] 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.

[43] 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).

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. The need to deal with the issues that can arise from having too much information in litigation may 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. 696, 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.[44]

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.

---

[44] The figures used are hypothetical and other approaches and cost figures would yield different results. The point is simply that the larger the volume of information the higher the costs will be in litigation, separate and apart from any substantive impact the information may have on the outcome.

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* Fed. R. Civ. P. 37(f)[45] ("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.")[46]; *Crandall v. City of Denver,* 2006 WL 2683754 at *2 (D. Colo. Sept.19, 2006) ("Mere existence of a document [in this case e-mail] destruction policy within a corporate entity, coupled with a failure to put a comprehensive "hold" on that policy once the corporate entity becomes aware of litigation, does not suffice to justify a sanction absent some proof that, in fact, it is potentially relevant evidence that has been spoiled or destroyed."); *Willard v. Caterpillar, Inc.,* 48 Cal. Rptr. 2d 607 (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 (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);[47] *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). *Cf. Optowave Co., Ltd. v. Nikitin,* 2006 WL 3231422 (M.D. Fla. Nov. 7, 2006) (failure to suspend normal retention policies, resulting in destruction of relevant evidence, following notice of possible litigation sufficient to warrant severe sanctions); *Aloi v. Union Pac. R.R. Corp.,* 129 P.3d 999, 1003 (Colo. 2006) (finding no need to show bad faith where documents intentionally destroyed in accordance with existing document retention policy, where party had notice of potential litigation and relevance of documents prior to destruction date).

---

[45] Fed. R. Civ. P 37(f) is anticipated to be renumbered as Fed. R. Civ. P. 37(e) effective December 1, 2007. *See* footnote 10, supra.

[46] The Advisory Committee Note to this amended Rule makes clear that "good-faith" includes proper implementation of a legal hold where necessary: "Good faith may require a party intervene to modify or suspend certain features of the routine operation of a computer system to prevent the loss of information, if that information is subject to a preservation obligation." Fed. R. Civ. P. 37(f) 2006 Advisory Committee Note. Although the amended Rule provides support for the contention that not all destruction of electronic information is spoliation, the Rule does not provide specific guidance as to what else defines "good faith," or what might constitute "exceptional circumstances" that would warrant sanctions. Further, the Rule does not prohibit a court from issuing sanctions under its own inherent authority, or under any other statutory authority. Accordingly, Rule 37(f) is not in and of itself a "safe harbor" so much as it is a general guideline.

[47] 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. See also *Greyhound Lines, Inc. v. Wade,* 2007 WL 1189451 *2 (8th Cir. 2007) ("The ultimate focus for imposing sanctions for spoliation of evidence is the intentional destruction of evidence indicating a desire to suppress the truth, not the prospect of litigation.")

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 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. *See* Comments 5.a, 5.b, and 5.e, below.

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.*, size limits 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 and fit their cultures, 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. *See also* Fed. R. Civ. P. 26(b)(2) 2006 Advisory Committee Note ("A party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence.")

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[48] 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.[49]

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, but may find it useful to do so in some instances.

Metadata[50] is sometimes referred to as "data about data." Metadata can come from a variety of sources: created automatically by a computer, supplied by a user, or inferred through a relationship to another document.[11] 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 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.

Metadata is created, modified and disposed of at many points during the life of electronic information, and in the ordinary course of business organizations routinely migrate information from one form to another affecting the metadata associated with those files. For instance, 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.

---

[48] The Glossary provided in the September 2005 publication of *The Sedona Guidelines* has been removed from this edition and readers are referred to *The Sedona Conference® Glossary for E-Discovery and Digital Information Management* (2d Edition) available at: www.thesedonaconference.org for the definition of these terms in order to ensure consistency in the definitions used throughout the Working Group's publications.

[49] The 2006 Amendments to the Federal Rules provide some safety for routine destruction of information done in good faith as part of an existing records management program, although these protections are not clearly defined. Fed. R. Civ. P. 37(f)("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."). But see note 5 above regarding limitations on this protection and open questions associated with Rule 37(f).

[50] According to ISO 1548-1, metadata is "data describing context, content, and structure of records and their management through time." *See also The Sedona Conference® Glossary for E-Discovery and Digital Information Management* (2d Edition) available at: www.thesedonaconference.org.

Absent a specific legal or business need, an organization need not retain the electronic version of a document and its associated metadata.[51] 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).

It should be observed that metadata includes contextual, processing, and use information which can assist with identification and certification of the scope, authenticity, and integrity of electronically stored information, including electronically stored records.[52] Because metadata may provide a wealth of information that can allow an organization to better retain and organize its information, organizations may find the retention and use of metadata to be beneficial from an organizational or operational perspective. Furthermore, organizations may wish to consider retaining sufficient metadata about records to ensure the trustworthiness of the records for organizational, fiscal, legal and historical purposes.[53] And many organizations employ information and records management programs that specifically use metadata tags to cull and organize information.[54] Finally, 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.

If an organization chooses to retain metadata in its normal course of business, it should be aware that the metadata may be discoverable in its complete and original form. *See, e.g., Williams v. Sprint*, 230 F.R.D. 640, 652 (D. Kan. 2005) (court ruled that presumption is in favor of producing metadata unless (1) producing party objects; (2) parties agree otherwise; or (3) court issues a protective order); *see also Nova Measuring Instruments Ltd. v. Nanometrics, Inc.*, 417 F. Supp. 2d 1121, 1122 (N.D. Cal. 2006) magistrate granted motion to compel defendant to produce electronic documents in native format with all original metadata, where defendant originally agreed to such production and provided no reason why it could not make such production); *In re NYSE Securities Specialists Litigation*, 2006 WL 1704447, at *1 (S.D. N.Y. June 14, 2006) (court ordered all electronic documents to be produced in native format,

---

[51] It is important to distinguish the ordinary situation from what might be required in a litigation context where an obligation to preserve metadata might be imposed. Organizations faced with the preservation obligations due to litigation or investigation and a desire to migrate information from one format to another should seek advice from competent legal counsel as to their obligations surrounding preservation relevant metadata. *See The Sedona Principles, Second Edition (2007), Principle 14* for additional guidance.

[52] 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.

[53] At the same time it should be recognized that too strict of reliance on metadata can cause anomalies in records and information management. For example, 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.

[54] *See e.g.*, the *Minnesota Recordkeeping Metadata Standard*, which is designed to support the accountability of government and the proper use of government records as mandated by law. The standard addresses many metadata elements, and other issues such as access restrictions, data practices, and records retention and disposition, thereby enabling the practical implementation of statutory mandates for records management. Use of the standard can: (a) facilite data sharing, (b) enhance efficiency with respect to locating, evaluating, and retrieving records, and (c) provide guidance to consultants, vendors, and system designers. The standard is comprised of ten mandatory and ten voluntary elements. It is referenced as a "current standard" in the Minnesota Enterprise Technical Architecture under Chapter 4, "Data and Records Management Architecture." See also http://metadata-stds.org/ (homepage of ISO/IEC JTC1 SC32 WG2, which is the Working Group within the ISO that develops international standards for metadata and related technologies); http://dublincore.org/ (The Dublin Core Metadata Initiative is an open organization engaged in the development of interoperable online metadata standards that support a broad range of purposes and business models. DCMI's activities include work on architecture and modeling, discussions and collaborative work in DCMI Communities and DCMI Task Groups, annual conferences and workshops, standards liaison, and educational efforts to promote widespread acceptance of metadata standards and practices); http://edrm.net/edrm_xml.php (Efforts of the Electronic Document Reference Model (EDRM) organization to develop XML Schema For Metadata); http://www.e.govt.nz/standards/nzgls/standard (The NZGLS metadata standard is the official New Zealand Government standard for creating discovery-level metadata (see Cabinet Circular CO (02) 3). The standard is based closely on two well-established standards: the Dublin Core Metadata Element Set and the Australian Government Locator Service.)

along with all associated metadata). See also Fed. R. Civ. P. 34(b) (allowing a requesting party to request electronically stored information in either the form "in which it is ordinarily maintained," or a form that is "reasonably usable"). *But see Williams v. Sprint/United Mgmt. Co.*, 2006 WL 3691604 (D. Kan. Dec. 12, 2006) (denying class action employment discrimination plaintiffs' request to require defendant to produce emails that transmitted certain spreadsheets in native format because plaintiffs had not provided sufficient reasons for requiring native production and defendant had raised convincing argument that redaction of privileged information was not technologically feasible in native format); *CP Solutions PTE, LTD. v. Gen. Elec. Co.*, et al., 2006 WL 1272615 (D. Conn. Feb. 6, 2006) (declining to order production of documents in native (.pst) format in a breach of contract and fraud case absent showing of need for a specific .pst file and a means to secure it without the production of privileged or irrelevant documents); *In re Priceline.com, Inc. Sec. Litig.*, 2005 WL 3465942 (D. Conn. Dec. 8, 2005) (directing that information be produced in non-native formats absent a showing that production of a file in its native format would be necessary to view or comprehend the information in the file).

Additionally, if in the ordinary course of business an organization migrates electronic versions with associated metadata to other versions without retaining 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. *See also The Sedona Principles, Second Edition* (2007), Principle No. 12 and Comment 12.a.

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), answers to FAQs, 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; and
- ***The organization's officer(s) or senior manager(s) for data security and privacy,*** who are responsible for compliance with federal, state and local laws relating to retention and destruction of personally identifiable information.

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: *See, Morgan v. U.S. Xpress, Inc.*, 2006 WL 1548029, at *5 (M.D. Ga. June 2, 2006) (adverse inference precluded summary judgment in favor of defendant where defendant destroyed backup tapes of satellite positioning records; company policy was to retain such backup tapes for two years, and relevant tapes were destroyed before the two-year period expired, but after litigation commenced); *DaimlerChrysler Motors v. Bill Davis Racing, Inc.*, 2005 WL 3502172, at *2-*3 (E.D. Mich. Dec. 22, 2005) (adverse inference ordered when defendant failed to institute a legal hold and destroyed e-mails as part of its regular retention and destruction policies); *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) rev'd and remanded on other grounds, —- So.2d ——, 2007 WL 837221 (Fla.App. 4 Dist. Mar. 21, 2007); *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 442 (S.D.N.Y. 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 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).[55] 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.

---

[55] *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).

> ***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).

> **Comment 4.e.**
> **An organization may wish to consider defining (formally or informally) the roles and responsibilities of employees regarding electronic information and records.**

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, defining the roles and responsibilities of employees regarding electronic information and records may improve an organization's control over its information and records. An electronic record may require different "custodians" throughout its lifecycle, just as different "custodians" may have different roles with respect to the development, implementation, and supervision of an information and records management policy. *See* Pat Franks and Nancy Kunde, *Why Metadata Matters*, The Information Management Journal, Vol. 40, No. 5 (Sept/Oct. 2006) (noting that it is common to see "representatives of information technology, business units, records management, and legal services" involved in the development of policies and procedures relating to electronic records).

Business unit or process owner employees may establish and maintain procedural controls to ensure that appropriate electronic records are created, received and retained to meet business and legal requirements. This may include the originator or recipient of an electronic record, or their successors in the business unit function, during the normal course of business activities. As the "content custodians" for electronic records they will address creation and preservation of the information from a business need and legal standpoint, and are responsible for authorizing the destruction of electronic information and records in accordance with approved retention schedule. They may also be responsible for preserving electronic information and records due to actual or reasonably anticipated litigation, government investigation or audit.

Technology custodians are generally responsible for the logistical and physical care of electronic records. Technology custodians 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.

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. Different aspects of electronic information create different issues for storing, maintaining and transmitting 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 for purposes of authentication, security, data integrity, search, retrieval and analysis. Metadata carries with it a number of considerations that are discussed here and in further detail in Comment 3.f, above. Metadata should be examined from the perspective of how it can benefit the organization in its ordinary and ongoing operations. 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, and in some types of records management systems, retaining

excessive metadata can needlessly increase costs of storage and complexity of a records management system. However, in many instances certain metadata fields may be invaluable resources to aid information and records management.[56] As noted in *Introduction to Metadata: Pathways to Digital Information, Online Edition, version 2.1*[57], published by the J. Paul Getty Trust, in the context of a network environment metadata can certify the authenticity and degree of completeness of the content of objects; establish and document the context of the content; identify and exploit structural relationships that exist between and within information objects; provide a range of intellectual access points for an increasingly diverse range of users; and provides some of the information an information professional might have provided in a physical reference or research setting. 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.[58]

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.

> ***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.

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.

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 ensure 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.

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,

---

[56] 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.

[57] Authored by Tony Gill, Anne J. Gilliland, Mary S. Woodley and Edited by Murtha Baca. *See* http://www.getty.edu/research/conducting_research/standards/intrometadata/index.html.

[58] In addition to the Getty publication referenced above, the Dublin Core Metadata Initiative may be useful to consider in evaluating what metadata elements are important to an organization's information and records management. *See* http://dublincore.org. The Dublin Core Metadata Initiative describes itself as an open organization engaged in the development of interoperable online metadata standards that support a broad range of purposes and business models. Additional resources may be found at http://www.mnhs.org/preserve/records/metadataresources.html.

many organizations publishing data on external (i.e., publicly accessible) web-based communication tools may not be fully aware of the metadata that may be viewed by individuals outside the organization and even captured and indexed by outside search engines. 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 .pdf or .tif can be used to remove certain metadata from the core document and to standardize the manner in which the document is maintained. Similarly, "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.

Electronic Archives: 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). 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 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.[59]

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.

---

[59] *See The Sedona Conference® Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery* (August 2007 Public Comment Version), *available at*: http://www.thesedonaconference.com/dltform?did=Best_Retrieval_Methods_revised_cover-and_preface.pdf; *see also 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.

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, records management or knowledge management ("KM") systems in-place.[60]

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.[61]

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). For guidance in developing policies for e-mail management and considerations for technological solutions, *see The Sedona Conference® Commentary on Email Management (August, 2007)* available at: http://www.thesedonaconference.org/content/miscFiles/Commentary_on_Email_Management___revised_cover.pdf.

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.

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.[62] 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.[63]

---

[60] The European Communities' "Model Requirements for the Management of Electronic Records" ("MoReq") distinguishes between a document management ("DM") and records management ("RM") system (equivalent to an electronic archive in this context) as follows:

DM System … Allows documents to be modified and/or to exist in several versions.	**RM System** … 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 business.	May support day-to-day working, but is also intended to provide a secure repository for meaningful records.

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 provide useful starting points for defining integration requirements.

[61] David Stephens and Roderick Wallace, *Electronic Records Retention: New Strategies for Data Life Cycle Management* (ARMA International 2003).

[62] 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.

[63] 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.

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.[64] 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).

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[65] 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.[66]

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.

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. 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.

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.[67] 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).

---

[64] 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.

[65] *Available at* http://www.iso.org. The two components of the standard are ISO 15489-1:2001 and ISO/TR 15489-2:2001.

[66] *Available at* http://www.arma.org; *available at* http://www.archives.gov.

[67] *Electronic Records Archives Concept of Operations* (CONOPS v. 4.0) § 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.

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.

Automated Tools[68]

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. *See The Sedona Conference® Commentary on Email Management (August, 2007)* available at: http://www.thesedonaconference.org. 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 need 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. Further, at least in federal court, one might rely on the provisions of Fed. R. Civ. P. 37(f) ("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."). However, it is important to note that the protection offered by this rule is limited. What constitutes "exceptional circumstances" or the "routine, good-faith operation of an electronic information system" is within the court's discretion, as is its ability to issue sanctions under its inherent authority to supervise discovery rather than '"under these rules." *See also, 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 and e-mail deletion was not suspended court barred witness from testifying at trial and imposed total sanctions of $2.75 million).

---

[68] This document is not primarily focused on the preservation, collection and production of information in the litigation context, however organizations may wish to consider what technology implementations from a records management context may assist (or impede) with litigation processes. Courts are increasingly less sympathetic to arguments that information is maintained in a form which makes it costly or burdensome to retrieve and produce in discovery. *AAB Joint Venture v. United State*s, 2007 WL 646157 at *11 (Fed. Cl. Feb. 28, 2007) (defendant's decision to transfer the e-mails to backup tapes did not exempt defendant from its obligations of production); *Linnen v. A.H. Robins C*o., No. 97-2307, 1999 WL 462015, at *6 (Mass. Super. Ct. June 16, 1999) ("To permit a party "to reap the business benefits of such technology and simultaneously use that technology as a shield in litigation would lead to incongruous and unfair results.")

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 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 §§ 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 addressing the privacy rights of individuals (*e.g., the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Gramm-Leach-Bliley Act of 1999*, and security breach legislation in 34 states) and their regulatory counterparts 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 determining the purposes and means of the processing of personal data, as distinguished from "data processors" defined as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller." 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.privacyinternational.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[69] 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.) Alternatively, U.S. companies can achieve "adequacy" for the purpose of transferring data from the EU by (a) gaining the consent of the data subject, (b) establishing "Binding Corporate Rules" between the EU data authority and the U.S. company, and (c) entering into contractual agreements using EU "Model Contracts" and "standard contractual clauses" (less favored by U.S. companies because the contracts require compliance with EU data protection law.)

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 of many possible approaches 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.

An organization is ultimately 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, an organization should carefully consider whether to apply its records retention policies to outside contractors, consultants and other third-party providers, when they have been delegated the responsibility for the creation, management, storage and disposition of information and records relative to those functions. Factors to consider include the extent to which the organization has out-sourced critical business functions (*e.g.*, Human Resources, Finance), the extent of independence

---

[69] On May 30, 2006 the European Court of Justice found that the EU did not have power under internal constitutional rules to enter into this agreement, and thus annulled this provision, effective September 30, 2006. http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/judgement_ecj_30_05_06_pnr_en.pdf
Efforts to create a new agreement were in process this summer. On October 6, 2006 the U.S. and EU struck a deal whereby the EU will "push" 34 pieces of information per passenger to the U.S. Department of Homeland Security. DHS will "facilitate" wider distribution within the United States, replacing the previous "pull" system that allowed US-direct access to EU passenger data. The new accord will expire at the end of July 2007. Negotiations regarding a permanent agreement are underway.

of the contractor, the extent to which such information is within the scope of legal holds, and the terms and conditions of the organization's contract with the third-party as it relates to the care, custody, control and ownership of the information and records.

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.[70] Circumstances that may require suspending normal destruction of electronic information and records would include, among others: actual or reasonably anticipated[71] litigation; government investigation[72]

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; *see also DaimlerChrysler Motors v. Bill Davis Racing, Inc.*, 2005 WL 3502172 (E.D. Mich. Dec. 22, 2005) ("Such normal procedures for destruction of documents must, however, be suspended when a party is on notice that they may be relevant to litigation, and the failure to make an adequate search of such documents before their destruction may be evidence of bad faith.")

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. 696, 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); *Consol. Aluminum Corp. v. Alcoa, Inc.*, 2006 WL 2583308 (M.D. La. July 19,

---

[70] *See The Sedona Conference® Commentary on Legal Holds (*August 2007 Public Comment Version), available at http://www.thesedonaconference.org/dltform?did=Legal_holds.pdf.

[71] 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.

[72] 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.

2006) (party should have reasonably anticipated litigation and suspended its regular document destruction policy when it sent a demand letter to the opposing party, even though complaint not filed until ten months later); *Aloi v. Union Pac. R.R. Corp.*, 129 P.3d 999, 1003 (Colo. 2006) (adverse inference instruction appropriate where party continued to destroy documents pursuant to its policy, even after being put on notice that litigation was likely via plaintiff's statement that he intended to file a lawsuit; evidence of specific bad faith not necessary); *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 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,, and Hynix Semiconductor, Inc. v. Rambus, Inc. 2006 WL 565893 (N.D. Cal. Jan. 5, 1006) (holding that the evidence did not show that Rambus adopted its policy in bad faith or targeted any documents with the intent to prevent production in a lawsuit).

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. 23, 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, Second Edition (2007)*.

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, Second Edition (2007)*, Principle No. 5. 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.*, 2003 WL 21997747, at *3 (S.D.N.Y. Aug. 22, 2003) (preservation obligations include backup tapes); *see also The Sedona Principles, Second Edition (2007)*, Comment 5.h.[73]

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).

> ***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 Crandall v. City of Denver*, 2006 WL 2683754 at *2 (D. Colo. Sept.19, 2006) ("Mere existence of a document [in this case e-mail] destruction policy within a corporate entity, coupled with a failure to put a comprehensive "hold" on that policy once the corporate entity becomes aware of litigation, does not suffice to justify a sanction absent some

[73] 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). *Cf. E*Trade Secs. LLC v. Deutsche Bank AG*, 230 F.R.D. 582, 592 (D. Minn. 2005) (because party "relied on its backup tapes to preserve evidence that was not preserved through a litigation hold, [the party] should have retained a copy of relevant backup tapes because it was the sole source of relevant evidence").

proof that, in fact, it is potentially relevant evidence that has been spoiled or destroyed."); *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 opposing party), *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 Computek Computer & Office Supplies, Inc. v. Walton,* 156 S.W.3d 217 (Tex. App. 2005) (protective order overturned as overbroad where it prohibited a party from routine destruction of information and records not related to issues in the lawsuit); *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* Fed. R. Civ. P. 37(f) 2006 Advisory Committee Note (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).

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. 23, 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 should 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).[74]

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 United Medical Supply Co., Inc. v. United States, 77 Fed. Cl. 257 (Fed. Cl. 2007)* (spoliation found where notice failed to reach relevant custodians due to incorrect e-mail addresses and attorney failed to follow up when no responses were received); *In re NTL, Inc. Sec. Litig.,* 2007 WL 241344 (S.D.N.Y. Jan. 30, 2007) (many employees did not receive legal hold notice, and those that did were not made aware of their continuing preservation obligations); *Consol. Aluminum Corp. v. Alcoa, Inc.,* 2006 WL 2583308 (M.D. La. July 19, 2006) (defendant's initial litigation hold did not include a sufficient number of employees, and the process failed to include consultation with a manager with knowledge of the employees and issues); *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 circulation by e-mail was not sufficient when many employees did not have access e-mail).

> ***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 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*, 229 F.R.D. 442 (S.D.N.Y. 2004) (recommending periodic re-issuing of litigation hold notices). But it is important to make sure that repeat notices are effective and that necessary follow-up or modification occurs. *See United Medical Supply Co., Inc. v. United States, 77 Fed. Cl. 257 (Fed.Cl. 2007)* (follow up notices were sent to same incorrect e-mail addresses as original notices and no follow-up occurred to ensure notice had been received and was being followed).

---

[74] 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); *cf. Consol. Aluminum Corp. v. Alcoa, Inc.,* 2006 WL 2583308 (M.D. La. July 19, 2006)(court found that subsequent notice, after receipt of initial discovery requests, to more employees than in the original notice was still insufficient because the hold should have included even more employees).

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).[75] 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*, 229 F.R.D. 442 (S.D.N.Y. 2004) (noting roles of counsel and client in implementing legal hold notices and procedures). Conversely, an inability to provide this information in conjunction with a failure to produce all relevant information could be damaging. *See Pioneer Res. Corp. v. Nami Res.Co., LLC*, 2006 WL 1635651 (E.D. Ky. June 8, 2006) (court ordered defendant to provide written documentation of its efforts to locate e-mail messages defendant claimed it could not find, noting failure to do so could result in sanctions).

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 in good faith 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.").

[75] Organizations should consider whether they intend to produce legal hold notices during discovery, keeping in mind that although legal holds may be withheld under privilege or work product protection even if relevant, such notices must be included on a timely and complete privilege log in order to maintain protection. *See Gibson v. Ford Motor Co.*, 2007 WL 41954 (N.D. Ga. Jan 4, 2007) (legal hold notices protected by attorney-client privilege); *Capitano v. Ford Motor Co.*, 2007 WL 586586 (N.Y. Sup. Ct. Feb. 27, 2007) (legal hold notices subject to work-product protection); *Kingsway Fin. Servs., Inc. v. Pricewaterhouse Coopers LLP*, 2006 WL 1520227 (S.D.N.Y. June 1, 2006) (legal hold notices relevant but privileged so long as they are included on a proper and timely privilege log).

The recognition of the availability of a "safe harbor" against culpability in such circumstances is essential, and the 2006 Amendments to the Federal Rules of Civil Procedure may provide some limited safe protection 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 Working Group believes that if an organization takes reasonable and good faith 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 should not be found to have engaged in "willful" misconduct. 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).

Cases

Statutes

Other Authorities

Rules

Treatises

Regulations

Appendix B: Resources & 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.]

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.

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

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.

Cohasset Associates, Inc.

- http://www.cohasset.com

Cohasset is a private consulting firm specializing in document-based information management, and is host to the Managing Electronic Records (MER) Conferences.

Committee on Institutional Cooperation (CIC), University Archivists Group (UAG)

- http://www.cic.uiuc.edu/groups/UniversityArchivistsGroup/
- http://www.cic.uiuc.edu/groups/UniversityArchivistsGroup/archive/BestPractice/UniversityArchivistsStandards.pdf

This website sets out CIC UAG Standards for an Electronic Records Policy.

Mint Business Solutions

- http://www.mintsolutions.co.uk/pages.asp?p=5

  The site provides solutions for document management and database/website development, including e-government.

- http://www.mintsolutions.co.uk/pages.asp?p=14

Records Management Links

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.

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.

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.

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.

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.icacds.org.uk/eng/standards.htm

ICA Committee on Descriptive Standards: Standards & Guidelines

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

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.

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.

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.

NAGARA (National Association of Government Archives and Records Administrators)

- http://www.nagara.org
- http://www.nagara.org/displaycommon.cfm?an=1&subarticlenbr=5

NAGARA is a professional organization dedicated to the effective use and management of

government information and publicly recognizing their efforts and accomplishments.

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

National Archives of Australia

- http://www.naa.gov.au
- http://www.naa.gov.au/recordkeeping/rkpubs/summary.html (links to record-keeping publications)

New South Wales State Records

http://www.records.nsw.gov.au/publicsector/erk/electronic.htm (electronic record-keeping)

OASIS

- http://www.oasis-open.org/home/index.php

Non-profit consortium coordinating development of e-business standards; parent organization for LegalXML.

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.

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.

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)

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.

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.

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.

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.

U.S. Department of Agriculture, Records Management

- http://www.ocio.usda.gov/records/index.html

Comprehensive web site with links to federal resources.

U.S. Department of Defense, 5015.2 Standard

- http://www.dtic.mil/whs/directives/corres/html/50152std.htm
- http://jitc.fhu.disa.mil/recmgt/p50152s2.pdf
- http://jitc.fhu.disa.mil/recmgt/dod50152v3_13jun06.pdf

Design Criteria Standard for Electronic Records Management Software Applications (June 2002) and Version 3 Exposure Draft (August 2006). 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.

U.S. Environmental Protection Agency (Records Management Website)

- http://www.epa.gov/records/policy/index.htm (contains links to additional sites)

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.

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.

U.S. National Archives and Records Administration

- http://www.archives.gov
- http://www.archives.gov/records_management/
- http://archives.gov/records-mgmt/initiatives/

Appendix C: Survey of Data Within an Organization

Includes E-Gov Electronic Records Management Initiatives and others.

- http://toolkit.archives.gov

  A rich resource of best practices documents on a range of issues affecting electronic records management, both in and outside of the federal government.

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.

Council of State Archivists (CoSA)

- http://www.statearchivists.org/states.htm

Comprehensive web site listing electronic record-keeping related resources including policies and programs from all 50 states.

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.

XML.ORG

- http://www.xml.org

XML standards for specific industry areas.

An organization's information and records management policy should be based on an accurate and complete understanding of the sources and types of electronically stored information 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 information and records management program: how information and records are created and maintained; how record disposition decisions are made and implemented; and how information and 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 electronically stored 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-mgmt/publications/records-management-self-evaluation-guide.html
- 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. Investigate the company's current state of information and records management

A. Obtain and review:

1. Any existing records management policies and directives (paper and electronic);
2. Any existing records retention schedules;
3. All information technology user policies and guidelines;
4. Any employee training materials or guidance documents relating to records management.

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?

III. Evaluate the Current State Documentation

A. Records management policy

1. Is it written?

2. Is it contained in a single document?

3. Is it clear?

4. Is it well distributed and easily accessible?

5. What is the scope of the policy?

6. Does it apply to all kinds of information? (*i.e.*, paper, e-mail, word processing documents, spreadsheets, databases, voice mail, instant messaging)

7. Does it apply globally?

8. Does it apply to subsidiaries and affiliates?

9. Does it apply to records in the possession of contractors, outside counsel, etc.?

10. Does it apply to all information, whether stored on site or offsite?

B. 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 information as "records" and other types of information 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 for that employee to seek clarification, and for the organization to rovide 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 records retention schedules or otherwise ommunicate 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?

C. Assess consistency of documentation

1. Is the records management policy consistent with the records retention schedules and any information technology policies?

2. Are the training materials and any other guidance given to employees consistent with the policies and schedules?

IV. Review how the organization implements its 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.

3. The status of shadowed or deleted information.

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 records 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, microfilming, or moving to another system), 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?

V. 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 electronically stored information 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?

4. How is historical electronically stored information managed? Does the organization retain information in-house, through third-party servers or vendors, or in another manner? Where is the information map showing what information is where?

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, removable drives, 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. Does the organization have a policy on forwarding of e-mail messages or content to accounts outside the organization, including employees' personal accounts (such as Yahoo! or other accounts that do not belong to the company)?

4. If the e-mail messages contain information which may be needed by others in the organization, how is this addressed?

5. Does the organization maintain or allow the use additional, outside or third-party based e-mail accounts? If so, is this true for all employees? What are the guidelines or restrictions on such accounts?

6. Can users access their electronic mail remotely (*i.e.*, from outside the office)? If yes, what connection options are available? Does a transaction record (*i.e.*, session log) exist to document access?

7. Are limits set on individual users' e-mail boxes? If so, what limits are set and how are they enforced?

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.)?

VI. 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 electronically stored information such as e-mail, files on servers, voice mail, etc.?

E. Evaluate the organization's historical records audits practices

1. Does the company have an audit program for records management?

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?

VII. 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. Who is responsible for monitoring and ensuring suspension compliance?
12. How long does it take to develop and issue an instruction to hold records?
13. What principles govern decisions as to the scope (years and varieties) of records that must be held?
14. Are suspended records held in the normal work area or sent elsewhere?
15. When the suspension ends and normal disposal can resume, how is that communicated?
16. What is done with records retained during a suspension once the suspension period has ended?

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 D: Working Group Participants Member & Observers

Woods Abbott
Raytheon Company

Ronni Abramson
King & Spalding LLP

E. Regan Adams
Goldman, Sachs & Co.

Sharon A. Alexander
Jones Day

Thomas Y. Allman

Keith Altman
Finkelstein & Partners LLP

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

James R. Arnold
KPMG

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

David Axelrod
Deloitte Financial Advisory Services LLP

John Bacevicius
Gartner, Inc.

Denise E. Backhouse
Morgan Lewis & Bockius LLP

Wanda Bailey
McGuireWoods LLP

Jennifer V. Baker
Navigant Consulting Inc.

Kimberly Baldwin-Stried Reich
KBS Consulting - Lake County Physicians Association

Craig Ball
Craig D Ball PC

Katherine L. Ball
Johns Hopkins University, Division of Health

Laura Bandrowsky
Duane Morris LLP

John A. Bannon
Schiff Hardin LLP

Theodore S. Barassi
Symantec Corp

Jerry F. Barbanel
Aon Consulting Inc.

Thomas I. Barnett
Sullivan & Cromwell

Jason R. Baron
National Archives and Records Admin.
Observer

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

Courtney Ingraffia Barton
Crowell & Moring LLP

Bobbi Basile
Ernst & Young LLP

Cynthia Bateman
Georgia Pacific Corporation

James A. Batson
Liddle & Robinson, LLP

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

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

Lawrence P. Bemis
Kirkland & Ellis LLP

Adam S. Bendell
Strategic Discovery Inc.

Steven C. Bennett
Jones Day

Kara Benson
Faegre & Benson LLP

Peter T. Berk
McDonald Hopkins LLC

Steven Berrent
Davis, Polk & Wardwell

Adam Beschloss
KPMG LLG

Richard E. Best
Action Dispute Resolution Services

R. Eric Bilik
McGuireWoods LLP

Joanna Blackburn
Starbucks Coffee Company

Daniel Blair
Bank of America

Stephanie Blair
Morgan Lewis & Bockius LLP

Matthew Blake
Franklin Data, LLC

Alan Blakley
RLS Legal Solutions

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

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

Hildy Bowbeer
3M

John J. Bowers
Womble Carlyle Sandridge & Rice PLLC

Kevin F. Brady
Connolly Bove Lodge & Hutz LLP

Richard G. Braman
The Sedona Conference
Ex Officio

Allison Brecher
Marsh & McLennan Co.

Julia Brickell
Altria Corporate Services, Inc.

Kelli J. Brooks
KPMG

Charlene Brownlee
Davis Wright Tremaine LLP

Greg Buckles
Consultant for Attenex Corporation

Macyl Burke
ACT Litigation Services

Patrick Burke
Guidance Software, Inc.

Chistine M. Burns
Cohasset Associates, Inc.

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

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

Kara Buzga
Milberg Weiss LLP

Jonathan S. Campbell
Capital One Services, Inc.

Mary Beth Cantrell
Amgen Inc.

Jacquelyn A. Caridad
Morgan Lewis & Bockius LLP

Diane Carlisle
Baker Robbins & Company

Scott A. Carlson
Seyfarth Shaw LLP

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

Jim Caspersen
Canadian Pacific Railway

Vincent Catanzaro
DuPont

Barbara Caulfield
Affymetrix, Inc.

M. Kate Chaffee
Faegre & Benson LLP

Lloyd B. Chinn
Proskauer Rose LLP

Thomas A. Clare
Kirkland & Ellis LLP

Michael A. Clark
EDDix LLC

Matthew Clarke
Ryley Carlock & Applewhite

R. Noel Clinard
Hunton & Williams LLP

Adam Cohen
FTI

Andrew M. Cohen
EMC Corporation

Matthew Cohen
Alix Partners

Sigmund J. Collins
Philip Morris U.S.A

Michael J. Conner
Deloitte Financial Advisory Services LLP

Clark R. Cordner
Orrick, Herrington & Sutcliffe LLP

Alfred W. Cortese Jr.
Cortese PLLC

Christopher V. Cotton
Shook Hardy & Bacon LLP

David Couzins
Wilmer Cutler Pickering Hale and Dorr LLP

Moze Cowper
Amgen Inc.

William Craco
Johnson & Johnson

Joyce Craig-Rient
Finnegan Henderson Farabow Garrett & Dunner LLP

Tim Crouthamel
State Farm Insurance Company

Conor R. Crowley
DOAR Litigation Consulting

John C. Cruden
United States Department of Justice
Environment and Natural Resource Division
Observer

Lorne W. Curl
Xact

Wendy Butler Curtis
Fulbright & Jaworski, LLP

Joseph Cvelbar
First American

M. James Daley
Redgrave Daley Ragan & Wagner LLP

Jonathan A. Damon
LeBeouf, Lamb, Greene & MacRae

Christopher M. Davis
Steptoe & Johnson LLP

Martha Dawson
K&L Gates

Robert J.C. Deane
Borden Ladner Gervais LLP

Daniel T. DeFeo
The DeFeo Law Firm, PC

John Paul Deley
Energy Information Administration
Observer

Radi Dennis
Sentry Consulting Group

Anthony J. Diana
Mayer, Brown, Rowe & Maw LLP

William B. Dodero
Bayer Corporation

John J. Dominguez
Berman Devalerio Pease Tabacco Burt & Pucillo

Paul F. Doyle
Proof Space

Phillip J. Duffy
Gibbons P.C.

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

Peg Duncan
Department of Justice, Canada
Observer

Troy Dunham
Cooley Godward Kronish LLP

Myron Eagle
Evidence Exchange

Victoria Edelman
LexisNexis Applied Discovery

Elizabeth F. Edwards
McGuireWoods LLP

Robert A. Eisenberg
Capital Legal Solutions

Laura E. Ellsworth
Jones Day

Todd Elmer
H5

Amor A. Esteban
Shook Hardy & Bacon LLP

Eric J. Evain
Connolly Bove Lodge & Hutz LLP

Cameron J. Evans
Honigman Miller Schwartz and Cohn, LLP

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

Arthur C. Fahlbusch
King & Spalding LLP

Mary Faria
Altria Corporate Services, Inc.

Jeffrey C. Fehrman
Onsite3

Joan E. Feldman
Navigant Consulting Inc.

Steve Fennell
Steptoe & Johnson LLP

Carmen Oveissi Field
Daylight Forensic & Advisory LLC

Kenneth Fields
Superior Court of AZ
Observer

Eric R. Finkelman
Ciba Specialty Chemicals Corporation

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

Jason B. Fliegel
Mayer Brown LLP

Ed E. Foster
Akerman Senterfitt

Thomas Freeman
Reed Smith LLP

Amy Freestone
Faegre & Benson LLP

Eric M. Friedberg
Stroz Friedberg LLC

Suzanne Frost
Faegre & Benson LLP

Thomas E. Gaeta
Navigant Consulting Inc.

Randy Gainer
Davis Wright Tremaine LLP

David J. Galbenski
Lumen Legal

James H. Gallegos
Burlington Northern and Santa Fe Railway

Victoria B. Garcia
New Mexico State Court System
Observer

Brendan Gardiner
Caterpillar, Inc.

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

Daniel B. Garrie
CRA International

Daniel K. Gelb
Gelb & Gelb LLP

Alan C. Geolot
Sidley Austin LLP

Anthony I. Giacobbe Jr.
Zeichner Ellman & Krause LLP

Stanley M. Gibson
Jeffer Mangels Butler & Marmaro LLP

Daniel C. Girard
Girard Gibbs LLP

Valentina Gissin
LeBoeuf Lamb Greene & MacRae

Edward Glynn
PricewaterhouseCoopers LLP

Richard Gomes
Citigroup

Dean Gonsowski
Xiotech, Inc.

James E. Gordon
Navigant Consulting Inc.

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

Richard Graham
Pension Benefit Guaranty Corporation
Observer

Ronald J. Green
Bank of America

Jay E. Grenig
Marquette University Law School

Ashley Griggs
EMC

Peter Gronvall
Adams Grayson

Joseph P. Guglielmo
Whatley Drake & Kallas LLC

Lisa Habbeshaw
O'Melveny & Meyers LLP

Matthew Hagarty
America Online, Inc.

Brian Hail
Haynes & Boone LLP

Julie Anne Halter

Lori A. Ham
Poyner & Spruill LLP

Jennifer Hamilton
Deere & Company

William F. Hamilton
Holland & Knight

Daniel J. Harbison
Connolly Bove Lodge & Hutz LLP

Earl Harcrow
Haynes & Boone LLP

Matthew S. Harman
King & Spalding LLP

Sherry B. Harris
Hunton & Williams LLP

Wes Harris
Shell Oil Company

Hope Haslam
Merrill Lextranet

Kris Haworth
LECG

Ronald J. Hedges
Nixon Peabody

Bruce Hedin
H5 Technologies

Michael Henga
Pillsbury Winthrop Shaw Pittman LLP

Peter C. Hennigan
Faegre & Benson LLP

William Herr

Michael Heyrich
Citigroup Inc.

Josephine H. Hicks
Parker Poe Adams & Beinstein

Cathy Hilf
McGuireWoods LLP

Hon. Timothy S. Hillman
United States District Court, Distirct of Massachusetts
Observer

Ted S. Hiser
Jones Day

Julie Hoff
Redgrave Daley Ragan & Wagner LLP

Robert Hoff
Wiggin and Dana LLP

W. Michael Holm
Womble Carlyle Sandridge & Rice PLLC

Tim Hood
Redgrave Daley Ragan & Wagner LLP

John Mathias Horan
Howrey LLP

Steve Horvath
Zantaz Inc.

Karen Hourigan
Redgrave Daley Ragan & Wagner LLP

Kelly Hoversten
Gray Plant Mooty

Geoffrey M. Howard
Bingham McCutchen LLP

Oleh Hrycko
H & A Computer Forensics

Stuart W. Hubbard
Schiff Hardin LLP

Tanya Hunter
Intel Corporation

Kenton J. Hutcherson
The Hutcherson Law Firm

David W. Ichel
Simpson Thacher & Bartlett LLP

Brian Ingram
Soloman Page Group LLC

David A. Irvin
Womble Carlyle Sandridge & Rice PLLC

Greg Jackson
The Hutcherson Law Firm

Conrad Jacoby
Attorney & Consultant

John Janes
Deloitte

Harvey Jang
Symantec Corp.

William R. Jenkins Jr.
Jackson Walker, LLP

John H. Jessen
Electronic Evidence Discovery, Inc.

Kevin F. Joerling
ARMA International

Deborah A. Johnson
Orchestria

Glenn Johnson
King & Spalding LLP

Mary Jo Johnson
Wilmer Cutler Pickering Hale and Dorr LLP

Megan Jones
Cohen Milstein Hausfeld & Toll, PLLC

Jeffrey J. Joyce
Kroll Ontrack

Deborah Juhnke
Blackwell Sanders Peper Martin LLP

Sidney Kanazawa
Van Etten Suzumoto & Becket LLP

Dr. Hironao Kaneko
Tokyo Institute of Technology
Grad. School of Decision Science/Technology

Gregory S. Kaufman
Sutherland Asbill & Brennan

Conrad S. Kee
Jackson Lewis LLP

Gaither Keener Jr.
Lowe's Companies, Inc.

William J. Kelleher III
Robinson & Cole LLP

Eleanor B. Kellett
Scana Services Inc.

John B. Kennedy
LeBeouf, Lamb, Greene & MacRae

Anne Kershaw
A. Kershaw PC, Attorneys and Consultants

Priya Keshav
Tusker Group LP

David J. Kessler
Drinker Biddle & Reath LLP

Laura M. Kibbe
Pfizer Inc.

Elizabeth Kidd
LexisNexis Applied Discovery

Dennis Kiker
Moran Kiker Brown PC

John K. Kim
Johnson & Johnson

Mike Kinnaman
Attenex Corporation

David Kittrell

Gene Klimov
DOAR Litigation Consulting

Melissa L. Klipp
Drinker Biddle & Reath LLP

Liane R. Komagome
Hewlett Packard

Steven S. Krane
Barton Barton & Plotkin LLP

Antigone Kriss
Chambers of Judge Kimberly Moore, United States Court of Appeals for the Federal Circuit
Observer

Joshua Kubicki
Solomon Page Group LLC

K.J. Kuchta
Forensics Consultation Solutions, LLC

James S. Kurz
Womble Carlyle Sandridge & Rice PLLC

Bradley R. Kutrow
Helms Mulliss & Wicker

Janet Kwuon
Reed Smith LLP

Francis Lambert
Zantaz Inc.

Edwin M. Larkin
Winston & Strawn LLP

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

Brandon Leatha
Electronic Evidence Discovery, Inc.

Brandon Lee
Deloitte Financial Advisory Services LLP

Edwin Lee
Stonebridge

R. Michael Leonard
Womble Carlyle Sandridge & Rice PLLC

Ronald J. Levine
Herrick Feinstein LLP

Pauline Levy
McDonalds Corporation

Robert Levy
Haynes & Boone LLP

Julie Lewis
Digital Mountain, Inc.

Paul Lewis
Protiviti

Thomas Lidbury
Mayer, Brown, Rowe & Maw LLP

Keith Lipman
Interwoven

Marie Lona
Winston & Strawn LLP

Joe Looby
FTI

Ralph Losey
Akerman Senterfitt

Cecilia Loving
Patterson Belknap Webb & Tyler LLP

Lorrie L. Luellig
Ryley Carlock & Applewhite

Patricia Clarke Lukens
Johnson & Johnson

Rosemary Lumpkins
Microsoft Corporation

James K. Lynch
Latham & Watkins LLP

Cecil A. Lynn III
Ryley, Carlock & Applewhite

Jessica J. Macarone
McCarter & English

Sheila Mackay
Daegis

Heidi Maher
Renew Data Corp.

Michelle Mahoney
Mallesons Stephen Jaques

Sheri Malec
McDonalds Corporation

Carrie Mallen
McKesson Corporation

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

Browning E. Marean III
DLA Piper

Robert Markham
Cohasset Associates, Inc.

David G. Martin
Medtronic, Inc.

Ann Marie Mason
Metropolitan Life Insurance Co.

Kathleen M. Massey
Motorola Inc.

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

Wayne Matus
Pillsbury Winthrop Shaw Pittman LLP

Tom Matzen
Xact

Kate Gordon Maynard
Robinson Bradshaw & Hinson

J.J. McCracken
Cooper Tire & Rubber Company

Anne B. McCray
McGuireWoods LLP

Gregory McCurdy
Microsoft Corporation

Michael McGuire
GMAC ResCap

Nancy McMahon
Department of Justice
Observer

William McManus
Ryley Carlock & Applewhite

Stephanie Mendelsohn
Genentech

James L. Michalowicz
ACT Litigation Services

Lucie Miller
Eli Lilly & Co.

Scott Milner
Morgan Lewis & Bockius LLP

Denise M. Mineck
Life Investors Insurance Company of America

Robert D. Moody
Berenfeld, Spritzer, Shechter & Sheer

Tim Moorehead
BP America, Inc.

Jack Moorman
PricewaterhouseCoopers LLP

Bill Morrison
Haynes and Boone LLP

Steve Morrissett
Finnegan Henderson Farabow Garrett & Dunner LLP

Helen Bergman Moure
K&L Gates

Shelia Murphy
Metropolitan Life Insurance Co.

Justin Myers
Rambus

Simon Nagel
Dechert LLP

Paul J. Neale Jr.
DOAR Litigation Consulting

Jon A. Neiditz
Locke Lord Bissell

John Nemazi
Brooks Kushman PC

Mollie Nichols
First Advantage

Jonathan Nystrom
Cataphora

John Oakley
Berenfeld, Spritzer, Shechter & Sheer

Kate O'Brien
Digital Mandate

Kate Oberlies O'Leary
General Electric Company

Timothy L. O'Mara
Latham & Watkins LLP

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

Patrick Oot
Verizon Communications Inc.

Timothy M. Opsitnick
JurInnov Ltd.

Greg Osinoff
Digital Mandate

Robert D. Owen
Fulbright & Jaworski, LLP

Laura Lewis Owens
Alston & Bird, LLP

Neil Packard
e-Diligent, Inc.

Deidre Paknad
PSS Systems Inc.

Danielle M. Panetta
Goodwin Procter LLP

Chris Paskach
KPMG

Robert W. Pass
Carlton Fields

Thomas Pasternak
DLA Piper

John Patzakis
Guidance Software

George L. Paul
Lewis & Roca LLP

Richard Pearce-Moses
Arizona State Library
Observer

Cheryl L. Pederson
Cargill Inc.

Peter Pepiton II
CA Inc.

Ginger Heyman Pigott
Reed Smith LLP

Justin David Pitt
Bass, Berry & Sims PLC

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

Vivian Polak
LeBeouf, Lamb, Greene & MacRae

Anthony (Tony) Polk
Electronic Evidence Discovery, Inc.

Lacelle Porter
LeBeouf, Lamb, Greene & MacRae

Ashish S. Prasad
Mayer Brown Rowe & Maw LLP

James Proscia
Brooks Kushman PC

Michael J. Prounis
Evidence Exchange

Harry Pugh
Citigroup, Inc.

Jennifer Quinn-Barabanov
Steptoe & Johnson LLP

Charles R. Ragan
Redgrave Daley Ragan & Wagner LLP

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

Donald C. Ramsay
Stinson Morrison Hecker LLP

Jonathan Redgrave
Redgrave Daley Ragan & Wagner LLP

Heather Reed
Capital One Services, Inc.

Jeffrey Reed

Sean Regan
Symantec

Daniel L. Regard
LECG

Mark V. Reichenbach
MetaLINCS

Anthony Reid
Deloitte Financial Advisory Services LLP

David Remnitz
FTI

Ann Marie Riberdy
Wilmer Cutler Pickering Hale and Dorr LLP

Mark (Rick) E. Richardson III
Glaxo Smith Kline

Mary K. Riley
Bank of America

John T. Ritter
Bank of America

Tyler Robbins
CaseCentral, Inc.

Karin A. Roberts
Eli Lilly & Co.

Paul M. Robertson
Redgrave Daley Ragan & Wagner LLP

William C.E. Robinson
GEICO Insurance Company

E. Casey Roche III
Discovery Mining Inc.

Michael S. Roe
Ashland Inc.

Dave Rogers
Ernst & Young LLP

John William Rogers
Perkins Coie LLP

Michael H. Rogers
Labaton Sucharow & Rudoff LLP

Herbert L. Roitblat
Orcatec LLC

Catherine Kane Ronis
Wilmer Cutler Pickering Hale and Dorr LLP

Matthew A. Rooney
Mayer Brown Rowe & Maw LLP

Andrea D. Rose
Crowell & Moring LLP

John J. Rosenthal
Howrey LLP

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

Alan J. Ross
Bricker & Eckler LLP

Ira P. Rothken
Rothken Law Firm

Charles Rothman
H & A Computer Forensics

Kenneth Rowe
Chief Security Officers

Jane K. Rushton
Prudential Financial

Harold J. Ruvoldt
Nixon Peabody LLP

Jay Safer
Locke Lord Bissell & Liddall LLP

Stuart K. Sammis
Corning Incorporated

Joseph R. Saveri
Lieff Cabraser Heimann & Bernstein, LLP

Leigh R. Schachter
Verizon Communications Inc.

Karen Schak
Deloitte

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

David Schieferstein
Philip Morris U.S.A

Ryan Schmelz
Riberian Enterprises Inc.

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

Eric J. Schwarz
Ernst & Young LLP

Dan P. Sedor
Jeffer Mangels Butler & Marmaro LLP

Steven Shankroff
Skadden ARPS

Jeffrey C. Sharer
Sidley Austin LLP

Jackson Sharman III
Lightfoot Franklin & White

Gregory Shelton
Williams Kastner & Gibbs PLLC

Robert W. Shely
Bryan Cave LLP

James D. Shook
EMC Corporation

David Shub
DiscoverReady

Mark Sidoti
Gibbons P.C.

Sonya L. Sigler
Cataphora, Inc

Tom J. Sikora
El Paso Corporation

Dominique Simard
Ogilvy Renault LLP

Robert R. Simpson
Shipman & Goodwin LLP

Julie Sinor
PricewaterhouseCoopers LLP

Amy Sipe
ACT Litigation Services

Peter B. Sloan
Blackwell Sanders Peper Martin LLP

Thomas J. Smedinghoff
Wildman, Harrold LLP

Arthur L. Smith
Husch & Eppenberger

Jessica Cullen Smith
McDermott Will & Emery

Ken Sokol
Electronic Evidence Discovery, Inc.

Catherine J. Sosso
Union Pacific Railroad Company

Carolyn Southerland
Huron Consulting Group

Mathew Spilka
Whatley Drake & Kallas LLC

Judith Starr
Pension Benefit Guaranty Corporation
Observer

Heidi Stenberg
Ernst & Young LLP

Cheryl Strom
McDonalds Corporation

Ariana J. Tadler
Milberg Weiss LLP

Steven W. Teppler

Jeffrey Teso
Steptoe & Johnson LLP

Jeane Thomas
Crowell & Moring LLP

Paul Thompson
Dartmouth College

Hon. Samuel A. Thumma
Maricopa County Superior Court, Arizona
Observer

Patrick Tofilon
Steptoe & Johnson LLP

Dan Torpey
Ernst & Young LLP

Christina (Tina) Torres
Microsoft Corporation

Robert W. Trenchard
Wilmer Cutler Pickering Hale and Dorr LLP

Gina Trimarco
McCarter & English

John Turner
AnaComp

Judy Van Dusen
VanKorn Group, Limited

Jason Velasco
Merrill Corporation

A. J. Venit
Bank of America

Peter Wacht
National Court Reporters Association

Jim Wagner
DiscoverReady

Lori Ann Wagner
Redgrave Daley Ragan & Wagner LLP

Vincent Walden
Ernst & Young LLP

Alston Walker
Stroock & Stroock & Lavan LLP

Kathryn Hannen Walker
Bass, Berry & Sims PLC

Skip Walter
Attenex Corporation

Paul L. Warner
Jeffer Mangels Butler & Marmaro LLP

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

Ryan Wasell
Weyerhaeuser Company

Shinjiro Watanabe
Steptoe & Johnson LLP

Ashley Watson
Attenex Corporation

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

Laurie A. Weiss
Fulbright & Jaworski, LLP

Brian Westenberg
Daimler Chrysler Corp.
Miller, Canfield, Paddock & Stone, PLC

David Wetmore
Ernst & Young LLP

David White
Seyfarth Shaw LLP

Maggie Whitney
Sidley Austin LLP

Robert B. Wiggins
Morgan Lewis & Bockius LLP

Jack Williams
Powell, Goldstein, Frazer & Murphy

James "Chuck" Williams
MetaLINCS

Robert F. Williams
Cohasset Associates, Inc.

David R. Wilson
DG Consulting LLC

Scott L. Winkelman
Crowell & Moring LLP

Thomas P. Wisinski
Haynes & Boone LLP

Kenneth J. Withers
The Sedona Conference
Ex Officio

Edward C. Wolfe
General Motors Corporation

Gregory B. Wood
Fulbright & Jaworski, LLP

Todd I. Woods
Lowe's Companies, Inc.

Sarah E. Worley
Pre-Trial Solutions, Inc.

Susan B. Wortzman
Wortzman Nickle Professional Corporation

Joel Wuesthoff
Ibis Consulting

Chris Yowell
Celerity Consulting

Jason Yurasek
Perkins Coie LLP

Patrick Zeller
Guidance Software

Appendix E: The Sedona Conference® Working Group Series & WGS℠ Membership Program

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

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

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

The first Working Group was convened in October 2002, and was dedicated to the development of guidelines for electronic document retention and production. The impact of its first (draft) publication—T*he Sedona Principles; Best Practices Recommendations and Principles Addressing Electronic Document Production* (March 2003 version)—was immediate and substantial. *The Principles* was cited in the Judicial Conference of the United State Advisory Committee on Civil Rules Discovery Subcommittee Report on Electronic Discovery less than a month after the publication of the "public comment" draft, and was cited in a seminal e-discovery decision of the Federal District Court in New York less than a month after that. As noted in the June 2003 issue of Pike & Fischer's *Digital Discovery and E-Evidence,* "The Principles...influence is already becoming evident."

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

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