

Records Management
Current Issues in Retention, Disposition and E-Discovery

David G. Ries
Thorp Reed & Armstrong, LLP
412-394-7787
dries@thorpreed.com

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. ELECTRONIC RECORDS	1
III. RECORDS MANAGEMENT AND RETENTION	5
A. Records retention considerations	8
B. Electronic Records – The Challenge:	10
C. Records management programs – Areas of coverage.....	12
D. Records management policies - Some specifics	12
E. Effective records management programs.....	13
F. E-mail Management.....	13
G. Electronic records – Challenges in deleting.....	14
H. Electronic records – Preserving integrity.....	14
I. Electronic records – Evidence issues	14
IV. DUTY TO PRESERVE AND SPOILIATION.....	15
A. Definitions and the Duty to Preserve	15
B. Spoliation and Sanctions.....	24
C. Recent High Profile Cases	24
V. E-DISCOVERY BASICS.....	27
A. Discovery Rules	27
B. The Federal Rules Amendments.....	28
C. State Guidelines	31
D. Unique Challenges Of Electronic Discovery	31
E. The E-Discovery Process.....	32
F. Allocation Of Expenses For Discovery Of Electronic Information.....	32
G. Form of Production	35
H. Use Of Consultants	38
I. Protection of Privilege	39
J. Conclusion	43
VI. ADDITIONAL INFORMATION SOURCES.....	44

I. INTRODUCTION

Records management, including creation, retention, continued access, and disposition (discarding and destruction), has been a major concern for businesses and organizations for years. The importance of effective records management has increased with the exponential growth in the volume of business records, particularly electronic records. Corporate records management policies and practices are now under great scrutiny in light of recent high profile incidents of document shredding and destruction. These incidents have created a new climate in which records preservation and disposition decisions will be judged more harshly from hindsight, sometimes resulting in severe sanctions like default judgments or adverse inference instructions. In addition, discovery of electronic records, including allocation of the substantial costs frequently associated with it, has become a major issue in litigation.

Development and implementation of an effective records management program is critical for businesses and organizations of all sizes. The alternative involves substantial risks, like loss of critical information, overwhelming litigation expense, or court sanctions like a default judgment.

II. ELECTRONIC RECORDS

The key development in recent years which has had a major impact on records and information management is the exponential growth of electronic records. It has been estimated that over 90 percent of records used in business today are electronically created and stored and as many as 90 percent of them exist only electronically, never making it to paper. Based on these estimates, only 10 percent or less of business records are created on paper.¹

¹ P. Lyman and H. Varian, *How Much Information 2003*, University of California, Berkeley.

What used to take file cabinets or numerous boxes to store can now be retained in compact electronic media. The reliance on electronic records is even greater for companies engaged in e-commerce and e-business because the nature of their business operations is almost exclusively electronic. Electronic data is different from paper in both volume and kind. There are often multiple copies dispersed in many locations. Significantly, digital data can be altered or lost from routine operation of information systems. In addition, digital records contain metadata – embedded electronic information beyond what shows up on a paper printout. Understanding these and other differences is important to an understanding of management of electronic data.

First, the potential volume of electronic records is great and often massive. The approximate storage capacity of text pages for the various electronic media are listed in the following table.

STORAGE CAPACITY²		
Medium	Capacity	Approximate Pages
Floppy Disk	1.44 MB	720 pages
Zip Disk	250 MB	125,000 pages
CD	650 MB	325,000 pages
Hard Drive (example-capacities vary) ³	40 GB	20,000,000 pages (500,000 / GB)

These page figures are approximate and will vary widely depending on software and format. Compression can increase capacity. Most modern programs generate a greater volume of data per page which will reduce these page counts. Graphics will also reduce page counts.

² See, M. Overly and C. Howell, *Document Retention in the Electronic Workplace* (Pike & Fischer 2001) at pp. 2-3.

³ For hard drives, the actual “pages” of data will be substantially lower. The operating system and applications take up a large amount of disk space.

In comparison, the typical file box used for records storage holds about 2,500 to 3,000 pages.⁴ Newer media, like DVDs and USB drives (also called “pen drives” or “thumb drives”), also provide for compact portable storage of large volumes of documents. As storage capacities have increased and costs of storage media have decreased, the volume of electronically stored information has grown exponentially.

E-mail has become the most common form of business and personal communication. It was estimated in 2005 that approximately 30 billion business e-mails were sent each day worldwide.⁵ Current estimates are substantially greater.

E-mail presents a particular challenge in records management and discovery because of its sheer volume and the number of copies of a single e-mail which generally exists in multiple locations. In addition, e-mail presents a risk because many users consider e-mail to be temporary or casual and include statements in e-mails which they would not otherwise put “in writing.” Permanence of e-mail presents a double risk: it cannot be relied upon where a permanent record is required (unless it is retained on paper or electronically) and it is very difficult to effectively eliminate an e-mail if someone wants to eliminate it.

A recent industry survey on electronic communications found, among other conclusions, that 70% of reporting companies use e-mail for negotiating contracts and agreements, 63% use it for discussing human resources issues, 84% use it for discussing operational or product strategies, and 71% use it for exchanging confidential communications.

⁴ A figure commonly used by litigation consultants for images of paper documents on a CD (which are different from electronic text documents) is 15,000 pages per CD.

⁵ IDC *Worldwide Email Message Forecast* (December 2005).

AIIM and Kahn Consulting, Inc., *Electronic Communications Policies and Procedures: A 2005 Industry Study*.

The continued rapid growth of electronic records will be advanced by the broad legal recognition of electronic transactions and electronic records in the federal Electronic Signatures in Global and National Commerce legislation, 15 U.S.C. §§ 7001-7031 (“E-Sign”) and the Uniform Electronic Transactions Act (“UETA”), and by the requirement that federal agencies generally recognize the validity of electronic submissions by October, 2003 (when practicable) in the Government Paperwork Elimination Act of 1998, 44 U.S.C. § 3504 nt.

One of the risks of electronic records is the ease with which they can be altered (either intentionally or inadvertently) and the difficulty in detecting alteration. This is a critical difference between paper and electronic data for purposes of e-discovery in litigation. Some electronic documents contain dynamic fields which automatically change without a user command. For example, the date in word processing documents is often set to change automatically to show the current date when the document is edited. In addition, documents are often linked to other documents so that entries in them automatically change when changes are made in the linked document. Documents can be post-dated or predated, recipients and cc lists can be changed and text and figures can be altered. E-mail can be “spoofed,” indicating a false sender and address. Finally, intentional alterations in electronic records are often difficult to discover without forensic analysis. It is important to consider the use of electronic discovery consultants and computer forensics consultants in appropriate cases – both for the party producing electronic evidence and for the party receiving it.

An important consideration with electronic records is that they contain more information than paper documents or printouts of electronic documents. The electronic format

contains “metadata,” i.e., “data about data,” which includes information about the electronic file such as when and by whom it was created, when and by whom it was edited, what changes have been made, when and by whom it was accessed, etc. Electronic records also often contain embedded data, like formulas in spreadsheets or links in databases, which does not appear in printed copies.

Electronic records, including e-mails, present particular challenges in records management and discovery because it is difficult to eliminate them, and because they reside in many locations: networks, desktop and laptops, hard drives, backup, PDAs, copies on CDs, disks, forwarded copies and ccs, etc.

Because electronic records can be easily altered, either intentionally or inadvertently, it is important to protect the integrity of records which are stored electronically and retrieved for litigation.

III. RECORDS MANAGEMENT AND RETENTION

Effective records management requires development and implementation of records management programs for paper and electronic documents, including (1) document and record creation (what should be and what should not be included in documents and receipt), (2) record distribution, (3) record storage (where and in what form records should be stored and access and availability during storage), and (4) retention periods (including when and how records should be discarded or destroyed). In parallel areas, policies and procedures on technology, Internet and e-mail usage, and information security are also important parts of an overall approach for companies and organizations.

Legal risk is a critical reason for establishing a records management program. In addition, legal considerations must be addressed in any records management program. While these legal aspects are important, records management is multidisciplinary – involving

management, business process, and information technology considerations in addition to legal issues. Although these other aspects are beyond the scope of this paper, they are essential to effective records management.

The two primary professional organizations which are dedicated to records and information management are ARMA International (the Association for Records Management Professionals), www.arma.org, and AIIM (the Association of Information & Image Management), www.aiim.org. These organizations provide publications, information and educational programs on records management. They also participate in the development of standards. ISO (the International Organization for Standards) has published standards for records management, including ISO 15489 (2001), *Information and Documentation – Records Management – Part 1: General and Part 2 – Information and Documentation* and ISO/TS 23081: (2004), *Information and Documentation – Records Management Processes – Metadata for Records*. The American National Standards Institute (ANSI), www.ansi.org, coordinates voluntary standards in the United States, including those developed by ARMA and AIIM. ANSI standards include record and information management standards. For example, ANSI approved ANSI/ARMA 8-2005, *Retention Management for Records and Information* in February of 2005. This standard covers general principles for structuring an information retention and disposition program. ANSI/ARMA 9-2004, *Requirements for Managing Electronic Messages as Records* was approved in October 2004.

In September 2005, the Sedona Conference released *The Sedona Guidelines for Managing Information and Records in the Electronic Age*. The report includes technical, legal and management guidelines for electronic records management. The Conference is a highly regarded research and educational institute which studies law and policy. In April 2007, the

group published its *Commentary On Email Management: Guidelines For The Selection Of Retention Policy*. In June, 2007, the group released *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production, Second Edition*, an updated version of its e-discovery principles. These reports are available at www.thesedonaconference.org.

A term of art which is frequently used in records management today is “information life cycle management.” It includes processes, procedures and technology to manage information flow within a business or organization, from its creation or receipt until final disposition. ARMA uses the term “recorded information management.” AIIM calls the process “enterprise content management.” Kahn Consulting, Inc., a recognized consultant in the field, uses the terms “Information Management” and “Information Management Compliance.” In records and information management, a distinction is made between “records,” which must be managed for business and legal reasons, and other information.⁶

Important initial steps in the information management process include conducting an inventory to determine the kinds of records or information created and used and developing a classification scheme for grouping records into classes. A records retention schedule is then prepared to set retention times for the various classes of records.

Records management and retention programs must address:

1. business needs
2. legal and regulatory record keeping requirements
3. legal documentation needs
4. litigation concerns.

⁶ R. Kahn and B. Blair, *Information Nation: Seven Keys to Information Management Compliance* (AIIM 2004), pp. 12-14; 17-29.

Records management programs should be tailored to the specific business or organization, with these four criteria in mind. As one recent article aptly explained it:

There is no cookie-cutter approach to creating an effective document retention policy. A sound policy must be tailored to fit the specific needs of the business involved and should have legitimate business purposes at its core. Rather than any desire to purge an occasional “smoking gun” from its files, the force compelling businesses to adopt appropriate document retention policies should be considerations of storage space and the administrative cost of searching through hundreds of boxes full of documents or massive electronic files to locate information.⁷

A. Records retention considerations

The fundamental business consideration in development of a records management policy for both paper and electronic records is the business needs which the company or organization will have for the records in the future, including who will need access to the records, how often, how quickly, and over what period of time. Records contain information which is a valuable asset of the business, including intellectual property, and it should be managed so that it is available and protected as long as it has value to the business.

Another important consideration is legal and regulatory requirements for record keeping under federal, state and local laws. These include requirements in legal areas such as tax laws, securities laws, employment laws, environmental laws, and many others. A helpful reference on federal requirements is CCH’s *Guide to Record Retention Requirements in the Code of Federal Regulations* which is updated yearly. Publications from organizations like the Association of Corporate Counsel and trade groups like the American Bankers Association are also excellent information sources.

⁷ J. Messina and D. Trinkle, “Document Retention Policies After Enron,” 46 *Boston Bar Journal* 18 (September-October 2002).

The next area of concern is legal documentation needs. This includes documents like deeds, titles, contracts and agreements, patents and similar documents which are likely to be needed for legal purposes, but may not be required under regulatory requirements.

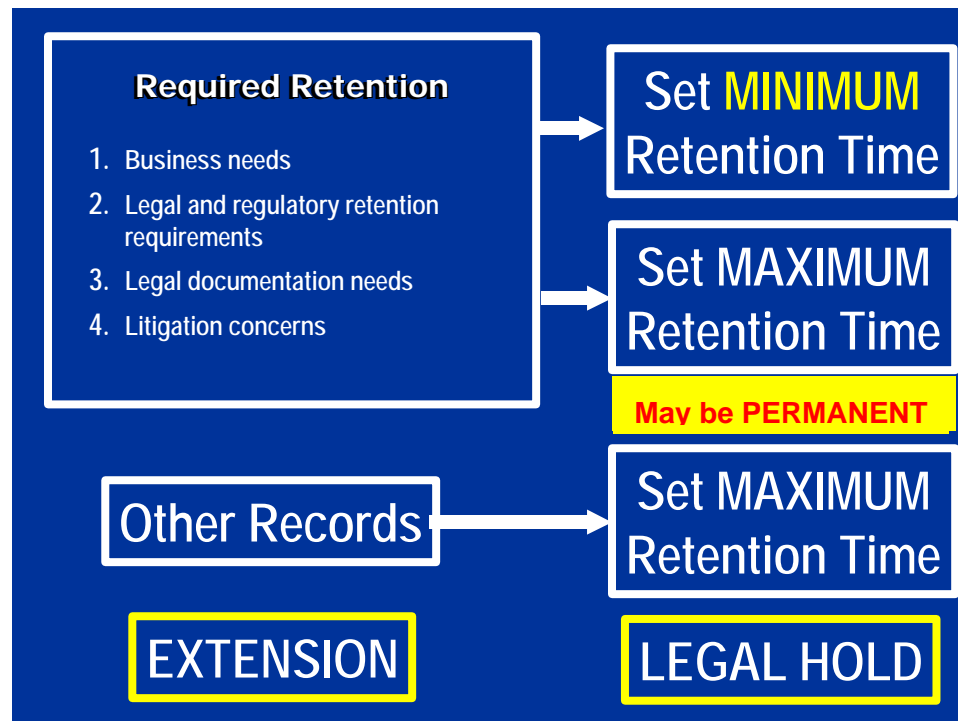
The fourth area in establishing a records management program is litigation considerations including (1) documents which may be needed to prove or defend a case and (2) documents which must be preserved under legal requirements to retain evidence for pending or anticipated litigation. Another important litigation consideration is the expense of retrieving and processing documents for litigation, particularly documents which have been retained beyond times required in document retention policies. Companies have frequently had to spend great effort and substantial amounts of money to process for litigation documents which should not have been retained under the company's record retention policy.

A program which effectively addresses these areas must be a joint effort of management, information systems, and legal counsel, as well as others in the business. It should be designed and implemented to work in the everyday work processes of the organization.

For records covered by these four categories (business needs, legal and regulatory retention requirements, legal documentation requirements and litigation needs), **minimum retention times** must be established. This will insure that records are available to satisfy these needs and requirements. For record control purposes, it is also generally advisable to set **maximum retention times** for documents covered by these four categories. For some records in these categories, like deeds, the retention time may be **permanent**. For documents outside of these categories, **maximum retention times** should be established for control purposes. A critical element in a records management program is a procedure to put a "**legal hold**" on destruction or discarding (potentially including backups) in the event of an investigation, audit,

claim or litigation. There also should be a procedure for permitting **other exceptions** to maximum retention periods.

These basic principles for a records management program are summarized in the following chart:



B. Electronic Records – The Challenge:

A 2003 survey found that 47% of the reporting organizations did not include electronic records in their record retention schedules, 59% did not have formal e-mail retention policies and 65% did not include electronic records in hold orders for inquiries and litigation.⁸ The survey’s conclusions included the finding “that for an alarming number of organizations, *the job of records management simply is not getting done.*” A 2005 update survey found significant

⁸ R. Williams, *Electronic Records Management Survey – A Call to Action* (Cohasset Associates, Inc. 2003).

improvement in many sectors.⁹ However, its conclusions included “...in the aggregate, *a great deal of further improvement is needed in the life cycle management of electronic records*” and “[w]hile many organizations have their act together,... *for an alarming number, the job of records management simply is still not getting done.*” A 2007 follow-up survey finds improvement and “a significant shift from awareness to action.” However, its conclusions include:

Most organizations have serious operational shortfalls regarding the processes by which they manage electronic records.

Some core deficiencies in records management program components have begun to be addressed – but the overall effectiveness with regard to life cycle management of electronic records remains bleak.

The number and magnitude of organizational and operational problems collectively represent stunning business risks.

Major gaps and risks related to the handling of archival and backup media remain.

The outstanding challenges associated with management of electronic information assets have the potential to be devastating in terms of cost, professional careers, and even corporate reputations.¹⁰

In a 2007 survey of corporate counsel, 61.7% reported that they were “dissatisfied” with their current corporate records policy and 6.3% reported that they were “extremely dissatisfied.” Significantly, less than 50% of responding corporate attorneys reported

⁹ R. Williams and L. Ashley, *Electronic Records Management Survey – A Renewed Call to Action* (Cohasset Associates, Inc. 2005).

¹⁰ R. Williams and L. Ashley, *2007 Electronic Records Management Survey: Call for Collaboration* (Cohasset Associates, Inc. 2007)

that their companies have the ability to enact hold orders [for investigations or litigation] accurately.¹¹

A 2006 survey highlights that e-mail management is not being effectively done in most organizations. Its “Key Finding #1” is:

For most organizations, “e-mail management” is usually something of an oxymoron, and at best more a wish than a business reality. Most organizations make heavy use of e-mail – it is the central means by which most business decisions are documented – yet most organizations continue to have a very casual attitude toward its management. E-mail started its life in most organizations as a proxy for conversation, and organizations largely continue to manage it in an ad hoc and casual way.¹²

C. Records management programs – Areas of coverage

Records management programs should cover the complete information life cycle

for both paper and electronic records, from creation to final disposition, including:

1. Creation
2. Distribution
3. Retention
4. Protection of trade secrets, confidentiality and privilege
5. Disposition (Discarding and Destruction)
6. Suspension of discarding and destruction in event of anticipated or pending investigation, claim or litigation – the legal hold process.

D. Records management policies - Some specifics

The program should be documented in a policy, as follows:

1. Written
2. Description of purpose and scope
3. Define responsibilities – many companies appoint a chief information officer or similar official to direct, but responsibilities of all officers, managers and employees should be defined.

¹¹ Jordan Lawrence Group, LC, *Survey of Corporate Records Practices 2006*, available at www.jordanlawrencegroup.com.

¹² John Mancini, *E-mail Management: An Oxymoron?* (AIIM 2006).

4. Description of coverage and exceptions
5. Define retention periods for covered categories of documents
6. Discarding or destruction: time, methods, responsibility and records (logs)
7. Provide for immediate suspension of discarding and destruction in event of investigation, claim or litigation, including preservation of electronic records.

E. Effective records management programs

A well prepared records management policy is only a part of an effective records management program. In addition to a policy, an effective program requires:

1. Implementation
2. Training
3. Enforcement
4. Auditing
5. Periodic review and revision.

F. E-mail Management

Technology solutions are being developed and implemented for management of e-mail. They include e-mail archiving tools for managing and preserving e-mail and analytic programs for searching archived e-mails. See, The Sedona Conference's *Commentary on E-mail Management: Guidelines for the Selection of Retention Policy* (April, 2007). A recent survey reports that the worldwide market for e-mail archiving applications grew by 45% in 2006 and is expected to approach \$1.4 billion in 2011.¹³

The Sedona *Commentary* describes the following typical features in use today for e-mail management:

1. User Mailbox Size Limitations ("Quotas")

¹³ IDG, *Worldwide E-mail Archiving Applications 2007-2011 Forecast and 2006 Vendor Shares: Storage Optimization, Mailbox Management, and Records Retention for eDiscovery and Compliance Drive Investments* (June 2007).

2. Automatic deletion of User Mailbox Contents (after a time duration, usually measured in days)
3. Extended Storage Options, and
4. Restrictions on Local Storage.

The *Guidelines* discuss the pros, cons, and legal aspects of these various approaches.

G. Electronic records – Challenges in deleting

Electronic records, including e-mails, present particular challenges because it is difficult to eliminate them, and because they reside in many locations: networks, desktops and laptops, hard drives, backup, PDAs, copies on cds, disks, forwarded copies and ccs, etc. In addition, **“Delete” does not mean it’s gone**. Most deleted files can be restored until the disk space in which they were stored has been overwritten. This does not happen when the “delete” command is used. However, software is available to manage electronic records and permanently delete data when secure disposal is necessary.

H. Electronic records – Preserving integrity

Because electronic records can be easily altered, either intentionally or inadvertently, it is important to protect the integrity of records which are stored electronically. Where appropriate, access should be limited and records should be stored in a “read-only” format.

I. Electronic records – Evidence issues

An important consideration in management of electronic records (and electronic images of paper records) is making sure that electronic records satisfy legal record retention requirements and will be admissible in legal proceedings. While Section 7001(a) and (d) of E-Sign and Sections 7 and 12 of UETA contain general provisions which recognize the legal sufficiency of electronic records, many questions still remain. For example, the Office of the

Comptroller of the Currency, on June 21, 2004, issued *OCC Advisory Letter AL 2004-9*, which cautions national banks concerning risks relating to electronic records because standards are still developing, including admissibility standards which may vary from state to state.

For an example of a case which excluded electronic records of a credit card account, *see, American Express v. Vinhnee*, 336 B.R. 437 (9th Cir. 2006). The court excluded the computer account records because it found that their authenticity had not been adequately established. The court provided a list of requirements for electronic records.

In the recent decision in *Lorraine v. Markel American Ins. Co.*, 2007 U.S. Dist. LEXIS 33020 (D. Md. May 4, 2007), the court provided a detailed analysis of the requirements for electronically stored information. Ruling on summary judgment, the court declined to consider emails offered by the parties because the foundation for their admissibility was not established. The court set out a roadmap of the necessary steps which should have been followed.¹⁴

In today's business and legal climate, there is no viable alternative to an effective records management program for both paper and electronic records. As discussed below, the risks of failure to address records management issues, including drastic legal consequences, are too great to ignore.

IV. DUTY TO PRESERVE AND SPOILIATION

A. Definitions and the Duty to Preserve

In preservation of evidence, it is critical to consider the dynamic nature of electronic data. While it generally takes some action to discard or destroy paper records,

¹⁴ *See*, Lexis Nexis, "*Lorraine v. Markel: Electronic Evidence 101*" available at www.lexisnexis.com/discovery.

electronically stored information can be lost through inaction. Routine operation of information systems containing the data can alter it and data is often automatically overwritten or deleted.

Spoliation is the intentional or negligent loss or destruction of evidence. A recent case defined “spoliation” as “the willful destruction of evidence or the failure to preserve potential evidence for another’s use in pending or future litigation.” Trigon Insurance Co. v. U.S., 204 F.R.D. 277, 284 (E.D. Va. 2001). Another recent case defined it: “[s]poliation includes the **intentional or negligent** loss of tangible and relevant evidence which impairs a party’s ability to prove or defend a claim.” West v. Goodyear Tire & Rubber Co., 167 F.3d 776 (2d Cir. 1999) (emphasis added).

Courts differ on whether intentional conduct or bad faith is necessary for sanctions for spoliation or whether negligence can lead to sanctions. Compare, Residential Funding Corp. v. DeGeorge Financial Corp., 306 F.3d 99, 101 (2d Cir. 2002) (adverse inference instruction “may be imposed where a party has breached a discovery obligation not only through bad faith or gross negligence, but also through ordinary negligence”); Stevenson v. Union Pacific Railroad Co., 354 F.3d 739, 746 (8th Cir. 2004) (“under either state or federal law – there must be a finding of intentional destruction indicating a desire to suppress the truth”); Beck v. Haik, 377 F.3d 624, 641 (6th Cir. 2004) (“spoliation is the intentional destruction of evidence,” without discussing negligence standard); and E*Trade Securities LLC v. Deutsche Bank AG, 230 F.R.D. 582 (D. Minn. 2005) (showing of bad faith is necessary for sanctions for destruction of relevant information before litigation has begun; no showing of bad faith is necessary where destruction of evidence occurs after litigation is imminent or has begun.)¹⁵

¹⁵ See, H. Chalmers, “Circuit Split Developing Over Requisite Level of Culpability for Adverse Inference Instruction,” *Litigation News*, September 2007.

Destruction of paper and electronic records under a proper records management policy is generally considered to be lawful where there is (a) no legal retention requirement and (b) no litigation or investigation, actual or reasonably anticipated. A recent article on document management notes that destruction under a valid document retention policy should generally be permitted without any adverse consequences:

. . . The destruction of hardcopy documents or deletion of electronic files pursuant to a valid document management program is clearly permissible and gives rise to no adverse inference if the documents are not available in subsequent litigation.

* * *

. . . While the standard that will be applied is one of “reasonableness” at the time of destruction (or nonpreservation), the issue will always be decided with the benefit of hindsight. . .¹⁶

The U.S. Supreme Court recognized the propriety of destruction under a valid document retention policy in the recent Arthur Andersen case:

“Document retention policies”, which are created in part to keep certain information from getting into the hands of others . . . are common in business. It is not wrongful for a manager or company to instruct its employees to comply with a **valid** document retention policy **under normal circumstances**.

U.S. v. Arthur Andersen, 125 S.Ct. 2129, at 2135 (2005) (emphasis added).

The Sedona Guidelines for Managing Information & Records in the Electronic Age (The Sedona Conference, September 2005) recognize destruction as an appropriate step in management of electronic records where there is no legal requirement for retention:

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

¹⁶ BNA, “Focus – Document Retention,” *Corporate Counsel Weekly* (February 20, 2002).

- 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.

One consideration in selecting the time for retention of records is the statute of limitations which applies to potential claims relating to the documents. A recent article summarizes this consideration as follows:

As a general rule, when a party destroys documents pursuant to routine procedures, no evidentiary presumption should be drawn about the destruction (assuming that the retention period is otherwise reasonable). Likewise, no evidentiary presumption may be appropriate when documents are destroyed after a period of years. Although there is no magic number, the term of retention should be *at least* as long as any applicable statute of limitations or regulatory review period. (Footnotes omitted.)¹⁷

Another consideration is the view that government agencies, courts, and juries may have toward the absence of records. While destruction may be legal under these legal standards and routine records management practices, they may still hold the absence of records against a business or enterprise which they believe should still have them.

¹⁷ I. Ballon, "Spoliation of E-Mail Evidence: Proposed Internet Policies and Framework for Analysis," *Cyberspace Lawyer* (March, 1999).

The duty to preserve relevant evidence arises when litigation or an investigation has commenced or is imminent, but may arise earlier. The obligation to retain arises when a “party has notice that evidence is relevant to litigation ... but also on occasion in other circumstances, as for example, **when the party should have known that the evidence may be relevant to future litigation.**” Byrnie v. Cromwell, 243 F.3d 93 (2d Cir. 2001) (emphasis added).

In addition to when preservation must start, there is also an issue of **what must be preserved**. When an investigation or litigation is started or anticipated, what is the scope of paper records and electronic data which must be preserved? A recent district court decision, Samsung Electronics Co., Ltd. v. Rambus, Inc., 2006 WL 2038417 (E.D. Va. 2006), describes the scope of the duty to preserve as follows:

Corporations are not obligated, “upon recognizing the threat of litigation,” to “preserve every shred of paper, every e-mail or electronic document, and every backup tape.” Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003). Indeed, “[s]uch a rule would cripple large corporations.” *Id.* Nevertheless, “[w]hile a litigant is under no duty to keep or retain every document in its possession..., it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request.” Wm. T. Thompson Co. v. General Nutrition Corp., Inc., 593 F.Supp. 1443, 1455 (C.D. Cal. 1984). “[A]nyone who anticipates being a party or is a party to a lawsuit must not destroy unique, relevant evidence that might be useful to an adversary.” Zubulake, 220 F.R.D. at 217.

The court later noted:

. . . Any company that implements a document retention policy during or in anticipation of litigation, and destroys documents relevant to the actual or anticipated litigation, will face and lose a spoliation charge. But that is as it should be.

Courts have noted that attorneys have the primary duty for preservation of evidence:

Once on notice, the obligation to preserve evidence runs first to counsel, who then has a duty to advise and explain to the client its obligations to retain pertinent documents that may be relevant to the litigation.

Telecom Int'l America, Ltd. v. AT&T Corp., 189 F.R.D. 76, 81 (S.D.N.Y. 1999).

In Zubulake v. UBS Warburg, LLC, 229 F.R.D. 422 (S.D.N.Y. 2004), the fifth decision on electronic discovery in an employment discrimination case, the court observed that the duty to preserve relevant records is the responsibility of both counsel and clients. Counsel first has the duty to notify the client to preserve relevant evidence, to locate relevant evidence and to ensure preservation. This is a continuing duty. "At the end of the day, however, the duty to preserve and produce documents rests on the party."

Zubulake states that counsel has a duty to ensure that "all sources of relevant information [are] discovered." It lists the following as the continuing steps which attorneys should take to comply with preservation obligations:

First, counsel must issue a "litigation hold" at the outset of litigation or whenever litigation is reasonably anticipated. The litigation hold should be periodically re-issued so that new employees are aware of it, and so that it is fresh in the minds of all employees.

Second, counsel should communicate directly with the "key players" in the litigation, *i.e.*, the people identified in the party's initial disclosure and any subsequent supplementation thereto. . . . [T]he key players should be periodically reminded that the preservation duty is still in place.

Finally, counsel should instruct all employees to produce electronic copies of their relevant active files. Counsel must also make sure that all backup media which the party is required to retain is identified and stored in a safe place. . . . One of the primary reasons that electronic data is lost is ineffective communication with information technology personnel. By taking possession of, or otherwise safeguarding, all potentially relevant backup tapes, counsel eliminates the possibility that such tapes will be inadvertently recycled.

229 F.R.D. at 433-434.

In a “Postscript,” the court states:

Now that the key issues have been addressed and national standards are developing, parties and their counsel are fully on notice of their responsibility to preserve and produce electronically stored information.

229 F.R.D. at 440.

The e-discovery amendments to the Federal Rules of Civil Procedure, which are discussed below, provide for a limited “safe harbor” for “electronically stored information lost as a result of routine, good-faith operation of an electronic information system.” Fed.R.Civ.P. 37(f). The rule provides limited protection from Rule 37 sanctions “absent special circumstances.” In Doe v. Norwalk Community College, 2007 WL 2066497 (D. Conn. July 16, 2007) the court held that, in order to take advantage of this provision in the face of pending or reasonably anticipated litigation, a party has a duty to act affirmatively to prevent the system from altering or destroying information.

In August 2007, the Sedona Conference published a Public Comment Version of its *Commentary on Legal Holds*, which explores preservation issues in detail.

The recent case, Phoenix Four, Inc. v. Strategic Resources Corp., 2006 WL 1409413 (S.D.N.Y. 2006), shows how far counsels’ duty can extend. This is a case against the plaintiff’s investment banker, alleging breach of fiduciary duty, common law fraud and negligent misrepresentation. Strategic Resources went out of business and closed its office before the litigation was filed. (The court found that it should have anticipated litigation at that time.) It left behind and abandoned 10 computer workstations at its office. The individual defendants took with them 2 servers and used them in their new business. In response to a document request, the defendants told their counsel “because SRC was no longer in operation, there were

no computers or electronic document collections to look through or search.” They did provide boxes of paper documents.

Within a few months, a freelance computer technician, who was working on one of the servers which was malfunctioning, discovered about 25 gigabytes of data in a dormant, partitioned section of the server – as much as 2,500 boxes of documents. The desktop computers in the new office could not access this data. A substantial production of this information was made at the end of the discovery period and it was necessary to take repeated depositions of some of the witnesses.

In addition to finding fault on the part of the clients, the court found that counsel had been grossly negligent in failing to conduct further inquiry concerning defendants’ representations that there was no electronic data. Counsel had a duty to conduct a “methodical survey” and “to search for *sources* of information.” Counsel should have asked what happened to the computers which were used at the closed office, which would have alerted counsel to the existence of the server.

When litigation or an investigation is initiated or anticipated, counsel should provide clients with clear, specific, written document preservation notices, including:

1. notice from counsel to management,
2. notice from counsel to key employees and IT personnel, with appropriate follow-up, and
3. notice from counsel to the adverse party to preserve its electronic evidence (should be considered).

The notices should include specific and detailed instructions about which paper and electronic records must be preserved and it should be communicated to everyone who may have control over the involved records. Appropriate follow up is necessary.

In analyzing document preservation issues in the context of litigation or potential litigation, it is important to note the broad scope of discovery under the Federal Rules of Civil Procedure and equivalent state rules. Fed.R.Civ.P. 26(b)(1) permits discovery not only of admissible evidence, but also of information “reasonably calculated to lead to the discovery of admissible evidence.” Determination of what should be preserved and what must be preserved presents a challenge, particularly for large and mid-size businesses, as information moves from that which is clearly relevant to that which is marginally relevant. The duty to preserve may be broader than the duty to produce. A court may decide that production of data is not required based on undue burden or expense. A failure to preserve deprives the court of the opportunity to make a decision.

An area which is sometimes overlooked is overwriting of backup tapes. In appropriate cases, it may be necessary to suspend this process.¹⁸ Preservation of electronic evidence presents a significant challenge because of its volume, the wide variety of types and the multiple locations where it might reside.

¹⁸ Standards as to whether and under what circumstances backup tapes must be preserved are still developing. Compare, *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production, Second Ed.* (The Sedona Conference 2007) p. 35, (“Absent specific circumstances, preservation obligations should not extend to disaster recovery backup tapes created in the ordinary course of business”); Zubulake v. UBS Warburg, LLC 220 F.R.D. 212, 217-18 (S.D.N.Y. 2003) (“As a general rule, then, a party need not preserve all backup tapes even when it reasonably anticipates litigation,” but preservation of backup tapes containing relevant evidence may be necessary. Generally, a litigation hold does not apply to “inaccessible backup tapes” “maintained solely for the purpose of disaster recovery,” but a hold would likely apply if they are “accessible” “i.e., actively used for information retrieval.”) and *7 MOORE’S FEDERAL PRACTICE* §37A.12[5][e] (“The routine recycling of magnetic tapes that may contain relevant evidence should be immediately halted on commencement of litigation”).

There is often no bright-line standard on when documents may be discarded or destroyed (in absence of a legal or regulatory requirement); it comes down to reasonableness of the policy and retention period under all of the circumstances. As discussed above, critical considerations in the analysis are pending and reasonably anticipated legal actions and statutes of limitations which would apply to claims related to the documents in question.

B. Spoliation and Sanctions

Courts have imposed harsh sanctions for spoliation of evidence, including dismissal of a case and entry of a default judgment. The range of potential sanctions for spoliation includes:

1. criminal prosecution – obstruction of justice, 18 U.S.C. §§ 1501, *et seq.* (enhanced by the Sarbanes-Oxley Act of 2002) and state statutes
2. dismissal or default judgment
3. contempt or penalty
4. preclusion of evidence, claim or defense
5. jury instruction – adverse inference from destruction or failure to produce witness or evidence
6. ethics violations for involved attorneys.

While courts consider a number of factors in determining an appropriate sanction for spoliation, the most important considerations are ordinarily (1) “the degree of culpability of the party who lost or destroyed the evidence” and (2) “the degree of actual prejudice to the other party.” *E.g., U.S. v. Koch Industries, Inc.*, 197 F.R.D. 488, 490 (N.D. Ok. 1999). Decisions dealing with sanctions are generally very fact specific and it is important to review them in context. The following cases are examples of the analysis which several courts have applied to spoliation issues.

C. Recent High Profile Cases

The harshest sanction for destruction of evidence is criminal prosecution for obstruction of justice. A recent example is the widely publicized prosecution of Arthur

Anderson in the Enron matter. Anderson was charged with destruction of paper and electronic records when it knew of Enron's financial problems and was aware of the likelihood of a federal investigation. The indictment charged:

... an unparalleled initiative was undertaken to shred documents and delete computer files. Tons of paper relating to the Enron audit were promptly shredded as part of the orchestrated document destruction. The shredder at the ANDERSEN office at the Enron building was used virtually constantly ... A systematic effort was also undertaken and carried out to purge the computer hard-drives and E-mail system of Enron-related files.

One of the issues in the case was an ambiguous notice from Anderson's counsel concerning compliance with Andersen's document retention policy which the government claimed was a signal to destroy records. Anderson was convicted of obstruction of justice and the conviction was recently affirmed on appeal. U.S. v. Arthur Andersen, LLP, 374 F.3d 281 (5th Cir. 2004), *rev'd* 125 S. Ct. 2129 (2005).

Arthur Andersen's conviction was reversed by the U.S. Supreme Court on May 31, 2005. However, the reversal was based on a jury instruction covering "knowingly corruptly persuad[ing]" another to "withhold" or "alter" documents for "use in an official proceeding," the required *mens rea*, and whether an ongoing official proceeding is necessary for a violation. While some observers point to the Supreme Court decision as an affirmation of reasonable pre-litigation or pre-investigation records retention policies, carried out in good faith, others point out that is based on a jury instruction for a criminal statute, which has now been expanded, and is likely to have little impact on sanctions in civil discovery. *E.g.*, ABAJOURNAL eReport, June 7, 2005 <http://www.abanet.org/journal/redesign/jn3ander/html>

The court imposed sanctions of preclusion of testimony and a monetary penalty of \$2,995,000 in U.S. v. Philip Morris USA, Inc., 2004 WL 1627252 (D.D.C. 2004). The court found that the employees of the defendant at the highest level violated both a court order and

their employer's document retention policies by deleting e-mails. The court noted that the defendant "is a particularly sophisticated corporate litigant which has been involved in hundreds, and more likely thousands of smoking-related lawsuits."

Another high profile example is Zubulake v. UBS Warburg, LLC, *supra*, 229 F.R.D. 422, in which the court found that sanctions of an adverse inference instruction at trial, costs of repeat discovery and costs of the sanctions motion would be imposed where the defendant willfully deleted e-mails after the court determined that they were relevant. Some of the e-mails were irretrievably lost while others were restored from backup after a number of months. In April 2005, after the adverse inference instruction was given at trial, a jury awarded \$9.1 million in compensatory damages and \$20.2 million in punitive damages.

As a final example, the court in Coleman Holdings, Inc. v. Morgan Stanley & Co., Inc., 2005 WL 679071 (Fla. Cir. Ct. 2005), *rev'd on other grounds*, No. 4D05-2606 (Fla. Dist. Ct. App., 3/21/07), instructed the jury to accept as established many of the allegations of the complaint which alleged that the defendant conspired to defraud the plaintiff in a major corporate acquisition. The court imposed this instruction as a sanction, based on findings of obstructionist behavior by the defendant during discovery, including failure to search approximately 1,400 backup tapes for e-mails and a false certification that a complete search had been made. After receiving the instruction on fraud, a jury, in May 2005, awarded \$604 million in compensatory damages and \$850 million in punitive damages, for a total of \$1.45 billion. In March, 2007, the judgment was reversed on damages issues, without ruling on the discovery sanctions. A dissent on the damages decision, which would remand the case, found the harsh discovery sanctions to be error.

V. E-DISCOVERY BASICS

Discover is the formal process under the court rules through which parties to litigation exchange relevant information and obtain information from third parties. In federal courts, discovery is governed by the Federal Rules of Civil Procedure. The respective states, including Pennsylvania, have their own discovery rules.

The time for a party to respond to interrogatories and requests for production is thirty days under Federal Rules 33(b)(2) and 34(b)(2)(A). The requesting party will generally agree to a reasonable extension, particularly for a large production. Courts will usually grant a reasonable extension where the parties do not agree. However, some courts have ordered aggressive production schedules which have included electronic data. A limited time for production can lead to substantial expense, particularly for a party which is not prepared in advance.

This section contains an overview of current issues in e-discovery. They are rapidly developing and new cases on these core issues are appearing every week. Because e-discovery law is rapidly developing, it is critical for attorneys and others working with e-discovery to have up to date information. Research on current developments should be conducted with sources like LEXIS and Westlaw, BNA's Digital Discovery & e-Evident (a newsletter and subscription site), <http://ddee.pf.com>, blogs like K&L Gates' e-discovery blog, www.ediscoverylaw.com, and websites of e-discovery service providers.

A. Discovery Rules

It is now beyond question that electronic information is discoverable. “[T]oday it is black letter law that computerized data is discoverable if relevant.” Anti-Monopoly, Inc. v. Hasbro, Inc., 1995 WL 649934 (S.D.N.Y. 1995).

Rule 34 of the Federal Rules of Civil Procedure has expressly provided for discovery of “electronic data compilations” since 1970 and electronic documents have been covered by the initial disclosure requirements of Federal Rule 26. Amendments to the Federal Rules of Civil Procedure which expressly address e-discovery became effective on December 1, 2006. They create a new category, of “electronically stored information” and provide special requirements and procedures for it.

It is also beyond question that electronic information is discoverable in Pennsylvania. Rule 4009.1 of the Pennsylvania Rules of Civil Procedure expressly covers “electronically created data, and other compilations of data from which information can be obtained, translated, if necessary, by the respondent party or person upon whom the request or subpoena is served through detection or recovery devices into reasonably useable form.”

B. The Federal Rules Amendments

In June 2004, the U.S. Judicial Conference’s Committee on Rules of Practice and Procedure published for public comment a series of proposed amendments to the Federal Rules of Civil Procedure to address electronic discovery issues. These amendments were approved by the full Judicial Conference in September 2005 and by the U.S. Supreme Court in April 2006. They became effective on December 1, 2006. The amendments apply to newly filed cases and, to the extent “reasonable and practicable,” to pending cases.

The amendments create a new category, of “electronically stored information” and provide for new procedures and requirements for it. Rule 34(a). Changes have been made to Rules 16, 26, 33, 34, 37 and 45. The new rules are available at www.uscourts.gov/rules/EDiscovery_w_Notes.pdf.

Some of the key changes include:

- Required early attention to electronically stored information, including (1) investigation by counsel of the client’s electronically stored information, (2) discussion at a Rule 26(f) “meet and confer” session and a Rule 16 court conference, and (3) electronic information is to be included in Rule 26(a)(1)(B) initial disclosures.
- The early attention covers discussion of privilege issues, including agreements and orders “for asserting claims of privilege or of production as trial preparation material after production.” Rule 16(b)(6) and 26(f)(4).
- Require that the recipient of privileged information which is inadvertently produced “may not use or disclose the information” and must “promptly return, sequester, or destroy the specified information and any copies” until the privilege issue has been resolved. Rule 26(b)(5)(B). (This is a procedural rule which does not determine the substantive law of privilege and waiver. See, the proposed amendment to Federal Rule of Evidence 502 and Hopson v. Mayor, 232 F.R.D. 228 (D.Md. 2005).)
- Require a showing of good cause by the requesting party to obtain electronic information which is “not reasonably accessible because of undue burden or cost.” Rule 26(b)(2).
- Address form of production by permitting the requesting party to specify the form or forms in which it is to be produced, subject to the responding party’s right to object. It must be produced “in a form or forms in which it

is ordinarily maintained or in a form or forms that are reasonably usable.”

Rule 34(b).

- Provide a limited “safe harbor” from Rule 37 sanctions for “electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.” Rule 37(f). (However, the scope of protection and the risk of sanctions based on other authority remain to be determined.)
- Provide for discovery of electronically stored information from nonparties through Subpoenas issued under Rule 45.

Significantly, these rules amendments do not provide new substantive requirements for preservation and retention of records and data. They provide for new definitions and procedures, including provisions that preservation issues should be addressed early, in the initial “meet and confer” and the initial Rule 16 Court Conference. The substantive requirements concerning what must be preserved and when the duty to preserve arises are set by statutes, regulations and case law, as discussed above.

This is a brief overview of the amendments. It is, of course, necessary to read the amended rules and comments for a complete understanding. In addition, two good sources of additional information are:

- C. Roberts, “The 2006 Amendments to the Federal Rules of Civil Procedure,” *Law Practice Today* (August 2006), available at <http://tinyurl.com/qbpdg> or www.abanet.org/lpm/lpt/articles/tch/08061.shtml (provides an overview of the new Federal Rules amendments)

- LexisNexis Applied Discovery, *Court Rules*, available at www.lexisnexis.com/applieddiscovery/lawLibrary/courtRules.asp#rules or <http://tinyurl.com/yedhzp> (provides a summary of the New Federal Rules Amendments.)
- G. Paul and B. Nearon, *The Discovery Revolution – E-Discovery Amendments to the Federal Rules of Civil Procedure* (American Bar Ass’n 2005) (provides a thorough treatment of the new Federal Rules amendments and their background)

C. State Guidelines

In August of 2006, the Conference of Chief Justices approved *Guidelines for State Trial Courts Regarding Discovery of Electronically Stored Evidence*. In August of 2007, the Uniform Law Commission approved *The Uniform Rules Relating to Discovery of Electronically Stored Information*. These uniform rules, like the uniform laws, provide the states with a model that is intended to achieve uniformity among the states. These guidelines and model rules, to a large degree, follow the same approaches as the federal rules amendments.

D. Unique Challenges Of Electronic Discovery

E-discovery presents a new series of challenges which require attorneys to understand their clients’ and adversaries’ information systems. There is a wide variety of types of digital data which has to be considered in e-discovery, such as: e-mails, data compilations, drafts, electronically created and stored documents, pictures, audio files, voicemails, Internet use records, and much more. This wide variety of electronic data resides on networks, computers and portable devices, often with multiple copies in different locations. Servers and network appliances often contain substantial information about how the network has been used, such as:

access to systems (log-ons/log-offs), access to programs/files, use of printers, faxes, etc., e-mail use and Internet use. Data is also frequently copied to backup media like backup tapes and mirror servers. This list is likely to continue to grow with advances in technology.

E. The E-Discovery Process

The e-discovery process includes the following steps:

1. Preservation
2. Collection
3. Processing (including filtering, deduplication, maintaining relationships between records, etc.)
4. Reviewing
5. Producing

Service providers can perform these steps or assist attorneys in performing them. It is, of course, necessary for attorneys to participate in reviewing for relevancy and privilege. Service providers make available powerful search tools, like conceptual searching, and provide hosting for large volumes of data which can be viewed and processed over the Internet.

Powerful search tools are now available for reviewing electronically stored information, both for analysis before production and for review by the recipients of production. They include such methodologies as keyword searching and conceptual searching, which relies on relationships between words and word patterns. These search tools can be used by businesses and organizations, outside counsel, and consultants. In August of 2007, the Sedona Conference published a Public Comment Version of a *Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*.

F. Allocation Of Expenses For Discovery Of Electronic Information

The costs of electronic discovery can be substantial, or even staggering, ranging from tens to hundreds of thousands of dollars and sometimes even more. Standards for allocation of these costs have been developing in the case law for the last several years and

patterns are emerging. While a detailed discussion of cost allocation and cost shifting is beyond the scope of this paper, it is a very important area for attorneys and parties to understand. A major case, Zubulake v. UBS Warburg, LLC, 217 F.R.D. 309 (S.D.N.Y. 2003), has been widely discussed as setting the standard for allocating expenses of electronic discovery. The opinion starts with the established presumption that the responding party must bear the cost of complying with electronic discovery costs and they may be shifted only when the discovery imposes an “undue burden or expense.” Generally, under this analysis, cost shifting is only considered for inaccessible data like backup tapes. The court established a 7 part test to determine whether some or all of the costs of production should be shifted:

specificity of the request,

1. availability of information from other sources;’
2. total cost – compared to amount in controversy
3. total cost – compared to relative financial resources of the parties,
4. relative ability and incentive to control costs,
5. importance of issues, and
6. relative benefits of information to the parties.

The court required the producing party to bear the cost of (a) producing the contents of optical disks, and (b) searching 5 sample back-up tapes for e-mails, with a later determination concerning additional information. After the sample review, the Court, in a later decision, required the producing party to bear 75% of the cost of restoring the back-up data and all of the cost of reviewing the back-up data for privilege. The requesting plaintiff was required to pay 25% of the cost of restoring the backup data. See, 216 F.R.D. 280 (S.D.N.Y. 2003)

In a case decided after Zubulake, a New York state court held that under New York law, the party seeking discovery of electronic data must bear the costs of production. Lipco Electric Co. v. ASG Consulting Corp., 2004 WL 1949062 (N.Y. Sup. Ct. 2004). A California state court ruled that the requesting party must bear the cost of obtaining data from

back-up tapes under a California procedural statute. Toshiba America Electronic Components, Inc. v. Superior Court, 2004 WL 2757873 (Cal. App. 2004).

The new federal rules make a distinction between data that is reasonably accessible and data that “is not reasonably accessible because of undue burden or cost.” Rule 26(b)(2)(B) provides:

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

Rule 26(b)(2)(C) includes the proportionality test – that the benefit of the proposed discovery must outweigh the burden and expense.

The “conditions” which the court may specify include a shift of some or all of the costs to the requesting party. The court may require that reasonably accessible data be produced and analyzed first, so that the need for data that is not reasonably accessible may be determined. Where production of inaccessible data is being considered, the court may provide for a sampling or phased production, so that the relevance and importance of the data can be reviewed on an ongoing basis rather than requiring production of everything in one step.

An example of the application of these new provisions is Ameriwood Industries, Inc. v. Liebman, 2007 WL 496716 (E.D. Mo. Feb. 13, 2007). The court found that a request for e-mails and computer files was overly broad, sought data that was not reasonably accessible, and production would be unduly burdensome. In Peskoff v. Faber, 240 F.R.D. 26 (D.D.C. 2007), one of several opinions in an ongoing e-discovery dispute, the court required the defendant to

conduct additional searches for e-mails, at its expense, because accessible data must be produced at the cost of the producing party.

For a detailed discussion of accessibility and costs under the new rules see, chapters 6 and 7 in G. Paul and B. Nearon, *Discovery Revolution – E-Discovery Amendments to the Federal Rules of Civil Procedure* (American Bar Ass’n 2007).

Because of the potential for substantial expense in discovery of electronic data, it is important to address cost-saving approaches early – either through agreement of the parties or involvement of the court. This can involve measures such as limiting locations to be searched, screening through automated searches, and phased searches for computer data.

G. Form of Production

An issue which has arisen in a number of cases is whether production of electronic records should be in electronic form or in the form of paper printouts of the records. Paper printouts are not the same as the electronic records because the electronic format contains metadata, i.e., “data about data,” (such as when and by whom the record was created, when and by whom it was edited, what changes have been made, when and by whom it was accessed, etc.). Metadata does not appear on printouts. In addition, electronic files like spreadsheets and databases contain embedded information which is not visible on paper printouts. Printed spreadsheets show only the final numbers, not the formulas by which they were calculated. Printouts of databases show only one alternative format for the information and do not have the search and sorting functions which are the essence of databases. This is an important consideration for both the producing party and the requesting party. In appropriate cases, it would be a serious mistake to ignore these attributes of electronic records. On the other hand, paper copies may contain notes, initials, highlighting, etc. which is not on electronic copies.

Under today's standards, production of electronic data will be electronic unless the parties agree on paper.

For electronic production, there is also an issue of the format of production, native or "locked" formats like TIFF or PDF. Native format is the format in which the file was created, like ".doc" for Microsoft Word. The format makes a difference on whether files can be altered (intentionally or inadvertently) and whether the records are computer searchable. There is also an issue of whether metadata and embedded must be produced. Where relevant, a computer searchable format, with metadata, can be important.

In Williams v. Sprint/United Management Co., 230 F.R.D. 640 (D. Kan. 2005), a significant recent decision, the court addressed the necessity of producing metadata. The court held that a party was required to provide metadata for spreadsheets where it had been ordered to produce electronic documents as they were maintained in the ordinary course of business. Plaintiffs wanted the metadata so that they could analyze the spreadsheet contents and perform their own calculations with the spreadsheets. Production of metadata would not be required if the producing party properly objected (in advance), the parties agreed that metadata would not be produced, or the producing party obtained a protective order.

In the recent decision in CP Solutions PTE, Ltd. V. General Electric Co., 2006 WL 1272615 (D. Conn.2006), the court required the defendant to re-produce electronic records in a "readable usable format" where the plaintiff claimed that the defendant engaged in "dump truck" discovery. The court did not require production of e-mails in native format.

The court found production of TIFF images to be inadequate in Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.I., 2006 WL 665005 (N.D. Ill. 2006). The court held that the TIFF format did not contain all of the relevant, nonprivileged information such as

modification dates, e-mail attachments and metadata. Courts have taken different approaches on these issues.

The federal rules amendments provide two alternatives for form of production of electronically stored information – “a form or forms in which it is ordinarily maintained” and “a form or forms that are reasonably usable.” Fed.R.Civ.P.34(b)(ii).

The request may specify the form or forms in which the data is to be produced. If it does specify the form(s), the responding party may either (a) produce the data in the requested form(s), or (b) object to the requested form(s) and state the form(s) which it intends to use. Fed. R.Civ.P.34(b). If the request does not specify a form(s), the written response must specify the form(s) which the responding party intends to use. Fed.R.Civ.P.34(b). That must be one of the alternative forms listed above. If the parties cannot agree on a form, the issue will have to be resolved by the court. If the requesting party does not request a form, it may be limited to the form(s) selected by the producing party.

Under this provision, the “form or forms in which it is ordinarily maintained” will usually be the native format in which the data was created like Microsoft Word or Excel. If the form is electronically searchable, the produced form must also be searchable. If metadata is relevant and a proper objection is not made to its production, metadata must generally be produced.

In the recent decision in Lawson v. Sun Microsystems, Inc., 2007 U.S. Dist. LEXIS 65530 (S.D. Ind. Sept. 4, 2007), the court required a second production in electronic form where the defendant produced hard copies and the plaintiff, in a letter, had requested an electronic form.

For more details on form of production under the new rules, see, Chapter 5 in G. Paul and B. Nearon, *The Discovery Revolution – E-Discovery Amendments to the Federal Rules of Civil Procedure* (American Bar Ass’n 2005).

H. Use Of Consultants

Consultants and service providers are helpful and generally necessary for addressing electronic discovery issues. There are two overlapping areas of expertise involved: electronic discovery services (collection and processing of electronic data) and computer forensics (acquisition, preservation and analysis of computer evidence - including searching for deleted and altered data, evidence of alteration, etc.). Since these are relatively new areas of expertise, it is important to carefully review the training, qualification and experience of consultants, including checking references. Because of the ease of altering, deleting and altering electronic data, it is important to retain a consultant early.

There are now reportedly over 500 companies offering e-discovery services. A recent article reports that e-discovery services is currently a \$2 billion market which is growing by 35 percent a year.¹⁹ A recent research report predicts that spending on e-discovery technology will reach \$4.8 billion by 2011.²⁰

The Sedona Conference has published *Navigating the Vendor Proposal Process: Best Practices for the Selection of Electronic Discovery Vendors* (The Sedona Conference 2007).

¹⁹ *Washington Post*, January 29, 2006, available at <http://www.washingtonpost.com/wp-dyn/content/article/2006/01/29/AR2006012900313.html> or <http://tinyurl.com/cek54>.

²⁰ Forrester Research, Inc., “Believe It – eDiscovery Technology Spending to Top \$4.8 Billion By 2011 (December 11, 2006).

It provides detailed guidance for selecting e-discovery service providers, including suggestions for requests for proposals.

I. Protection of Privilege

Protection of attorney-client privilege and work product is one of the paramount considerations in e-discovery.

Elements

While the elements of attorney-client privilege are stated somewhat differently in different jurisdictions, the following elements are generally included:

1. a communication,
2. made between privileged and persons,
3. in confidence,
4. for the purpose of seeking, obtaining or providing legal
5. assistance to the client,
6. affirmatively asserted and not waived.²¹

Corporations

The U.S. Supreme Court in Upjohn Co. v. United States, 449 U.S. 383 (1981) held that the attorney-client privilege applies broadly to corporations based on a subject matter test and is not limited to those in the corporation's control group. Under Upjohn, corporate communications are privileged if:

1. made by corporate employees,
2. to counsel for the company, acting as counsel, at the direction of corporate superiors,
3. concern matters within the scope of the employee's duties,

²¹ E. Epstein, *The Attorney-Client Privilege and the Work Product Doctrine*, 4th ed. (American Bar Association 2004 Supp.) at pp. 45-46.

4. to secure legal advice; and
5. considered confidential and so maintained.

Id. at 394-395.

Covered communications to the attorney generally have broad protection.

Depending on the jurisdiction, communications from the attorney to the client may be broadly protected or may not be protected if they do not disclose confidences received from the client.

Work product

Work product is a qualified protection, codified in Rule 26(b)(3) of the Federal Rules of Civil Procedure, which protects from discovery in civil cases:

1. documents and tangible things,
2. prepared in anticipation of litigation or for trial,
3. by or for another party or by or for that other party's representative (including the other party's attorney or consultant...).

Work product protection applies in a litigation context only and does not generally apply to legal services outside of disputes or litigation. It also generally terminates when the litigation ends. It is qualified because it can be overcome by a showing of substantial need for the information and inability to obtain it without undue hardship. Work product protection in criminal cases is provided by Rule 16 of the Federal Rules of Criminal Procedure.

Waiver by intentional production

While some courts have recognized a selective waiver of privilege by production of information to a government agency, there is a substantial risk that production to the government, even under a confidentiality agreement, will be a general waiver of privilege.

Compare, In re Columbia/HCA Healthcare Corp. Billing Practices Lit., 293 F.3d 289 (6th Cir. 2002) (disclosure of privileged information to the government waives privilege as to all other parties; agreeing with the First, Third, Fourth and D.C. Circuits) with Diversified Industries v.

Meredith, 572 F.2d 596 (8th Cir. 1978) (en banc) (voluntary compliance with a government subpoena does not waive privilege in subsequent litigation).

Inadvertent disclosure

Courts have taken varied approaches to the effect that inadvertent disclosure will have on privilege, ranging from strict waiver from inadvertent disclosure, to a balancing test, to no waiver absent client consent.²²

Response by recipient of inadvertent disclosure

ABA Formal Opinion 92-368 (1992) (withdrawn 2005), *Inadvertent Disclosure of Confidential Materials*, (withdrawn 2005), reaches the conclusion that:

A lawyer who receives materials that on their face appear to be subject to the attorney-client privilege or otherwise confidential, under circumstances where it is clear that they were not intended for the receiving lawyer, should refrain from examining the materials, notify the sending lawyer and abide the instructions of the lawyer who sent them

A recent amendment to Rule 4.4 of the ABA Model Rules of Professional Conduct accepts only part of this opinion and provides:

- (b) A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.

This amendment to the Model Rules will take effect in the various states only if they adopt it.

Pennsylvania has adopted this amendment.

State privilege law

²² Id. at 309-316.

This discussion of attorney-client privilege and work product is generally based on federal law. It is critical to consult state statutes, rules and court decisions on privilege where state law governs.

Attorney-client privilege in Pennsylvania is governed by statute, 42 Pa. Cons. Stat. § 5928. Pennsylvania law on attorney-client privilege is generally the same as federal law. See, Brennan v. Brennan, 422 A.2d 510 (Pa. Super. 1980), Rhone-Poulenc Rorer, Inc. v. Home Indemnity Co., 32 F.3d 851 (3d Cir. 1994) (finding nothing unusual or peculiar in Pennsylvania law of attorney-client privilege). Work product protection in Pennsylvania is governed by Rule 4003.3 of the Pennsylvania Rules of Civil Procedure. Under this rule, work product protection for materials prepared by clients and by representatives of clients other than attorneys, is much narrower than under the federal rules. In addition, under Pennsylvania Rule 4003.4, witness statements are not protected as work product (in contrast to federal Rule 26 which generally protects witness statements).²³

In Carbis Walker, LLP v. Hill, Barth and King, LLC, 2007 WL 2080599 (Pa. Superior, 7/23/07) the Pennsylvania Superior Court adopted the intermediate approach in a case where a law firm sent a fax intended for its client to opposing counsel. Despite adopting the intermediate approach, the court found a waiver of privilege, based on counsel's 18-day delay in requesting return of the fax.

Protection of privilege

Electronically stored information presents a substantial risk of waiver of attorney-client privilege and work product because of its volume and often unstructured content. It is

²³ See generally, K. Allen, *The Attorney-Client Privilege in Pennsylvania* (Pennsylvania Bar Institute 2007).

often very difficult and expensive to locate and review potentially privileged records which may be distributed among thousands or hundreds of thousands of records, or even more. One approach in addressing this challenge has been nonwaiver agreements or “claw back” agreements which provide that there will be no waiver in the event of inadvertent production. These agreements are sometimes included in protective orders. This approach is recognized in the proposed amendments to the Federal Rules. However, there are questions concerning the scope of protection provided by these kinds of agreements and orders, and the nature of review which still needs to be performed before production. For a recent opinion which discusses these issues, see Hopson v. Mayor, 232 F.R.D. 228 (D.Md. 2005).

There is a proposed amendment to Federal Rule of Evidence 502 concerning attorney-client privilege and work product. This amendment addresses nonwaiver agreements and orders to protect against inadvertent production of privileged materials. It generally provides that agreements are enforceable between parties and orders are enforceable against parties and nonparties. This amendment is proceeding through the rulemaking process and is not part of those which took effect in December 2006.

J. Conclusion

Records management is a critical concern today for businesses and organizations of all sizes. The alternative involves substantial risks, including loss of critical information, overwhelming expense in litigation, and harsh sanctions imposed by courts. It is particularly important to have a process in place for implementing a legal hold for pending or reasonably anticipated litigation and investigations.

VI. ADDITIONAL INFORMATION SOURCES

Records Management

AIIM International (Association of Information & Image Management), www.aiim.org/ (a professional organization focusing on document management, content and business processes)

American National Standards Institute (ANSI), ANSI/ARMA 8-2005, *Retention Management for Records and Information*.

American National Standards Institute (ANSI), ANSI/ARMA9-2004, *Requirements for Managing Electronic Messages as Records*

Association of Corporate Counsel and Jordan Lawrence Group, *Records Retention InfoPAK* (2006)

Association of Corporate Counsel, *Leading Practices in Information Management and Records Retention: What Companies are Doing* (2003)

ARMA International (the Association for Records Management Professionals), www.arma.org/ (a professional organization in the field of records and information management, providing education and research and creating best practices and standards)

M. Brown and P. Weiner, "Digital Dangers: A Primer on Electronic Evidence in the Wake of Enron," *Litigation* (Fall 2003)

CCH, *Guide to Record Retention Requirements in the Code of Federal Regulations* (2006) (updated yearly)

R. N. Cogar and R.T. Howell, "Retention: More Important Than Ever," *Business Law Today* (September/October 2003)

G. Cunningham and J. Montana, *The Lawyer's Guide to Records Management and Retention* (American Bar Ass'n 2006)

P. French, "Electronic Document Retention Policies (And Why Your Clients Need Them)," *Law Practice Today* (January 2004)

R. T. Howell, Jr. and R. N. Cogar, "Developing And Implementing A Record Retention Program," *The Practical Lawyer* (December 2004)

International Organization for Standards (ISO), ISO 15489:2002, *Information and documentation – Records management* and ISO/TS 23081: 2004, *Information and documentation – Research management processes – Metadata for records*

Iron Mountain, *Records Management: A Practical Approach to Building a Comprehensive and Compliant Records Management Program* (2005)

B. Jameson, "Document Retention and Electronic Discovery," *The Practical Litigator* (September 2004)

Jordan Lawrence Group, *Survey of Corporate Records Practices 2006*, available at www.jordanlawrencegroup.com.

R. Kahn and B. Blair, *Information Nation: Seven Keys to Information Management Compliance* (AIIM 2004)

R. Kahn and B. Blair, *Information Nation Warrior: Information Management Compliance Bootcamp* (AIIM 2005)

Jordan Lawrence Group, *Survey of Corporate Records Practices 2006*

S. Nelson and J. Simek, "Law Firm Document Retention Policies," *Law Practice Today* (July 2004)

M. Overly and C. Howell, *Document Retention in the Electronic Workplace* (Pike & Fischer 2001)

W. Saffady, *Digital Document Management* (ARMA International 2007)

W. Saffady, *Managing Electronic Records, 3d Ed.* (ARMA International 2002)

W. Saffady, *Records and Information Management: Fundamentals of Professional Practice* (ARMA International 2004)

The Sedona Guidelines for Managing Information & Records in the Electronic Age (The Sedona Conference, September 2005), available at www.thesedonaconference.org

T. Smith and W. Dodera, "Creating a Strong Foundation for Your Company's Records Management Practices," *ACC Docket* (November 2007)

D. Stevenes, *Records Management: Making the Transition from Paper to Electronics* (ARMA International 2007)

West Corporate Compliance Series, Vol. 3, *Designing an Effective Record Retention Program* (2005 Supp.)

R. Williams, *Electronic Records Management Survey – A Call To Action*, (Cohasset Associates, Inc. 2004) available at www.cohasset.com

R. Williams and L. Ashley, *Electronic Records Management Survey – A Renewed Call To Action*, (Cohasset Associates, Inc. 2005) available at www.cohasset.com

R. Williams and L. Ashley, *Electronic Records Management Survey – Call for Collaboration*, (Cohasset Associates 2007) available at www.cohasset.com.

R. Williams, *Realizing the Need and Putting the Key Components in Place to “Getting it Right” in Records Management* (Cohasset Associates, Inc. 2002) available at www.cohasset.com

E-Discovery

Applied Discovery, Inc., <http://www.applieddiscovery.com/> (a LexisNexis company; provider of electronic discovery services – website contains articles, links, and case summaries, publishes *The E-Discovery Standard*, a free quarterly newsletter)

M. Arkfield, *Electronic Discovery and Evidence* (Law Partner Publishing 2006-2007 ed.) (a looseleaf treatise, periodically supplemented)

C. Ball, *Six on Electronic Data Discovery*, (6 articles including such areas as the new e-discovery rules, metadata, and preservation letters). These and other materials are available at www.craigball.com

BNA, *Digital Discovery & e-Evidence* (a monthly report and Internet reference service) <http://www.pf.com/ddeePD.asp>

M. Brown and P. Weiner, “Digital Dangers: A Primer on Electronic Evidence in the Wake of Enron,” *Litigation* (Fall 2003)

A. Cohen and D. Lender, *Electronic Discovery: Law and Practice* (Aspen 2007 Supp.) (a looseleaf treatise, periodically supplemented)

Conference of Chief Justices, *Guidelines For State Trial Courts Regarding Discovery of Electronically-Stored Information* (Approved August 2006)

W. Cowan and K. Abboa-Offei, “A Practical Guide to Conducting Electronic Discovery,” *The Practical Litigator* (January 2005)

Discovery Resources, www.discoveryresources.org/ (electronic discovery resources for legal professionals)

Federal Judicial Center, *Manual for Complex Litigation (Fourth)* (2004) § 11.446, “Discovery of Computerized Data”

J. Feldman, *Essentials of Electronic Discovery: Finding and Using Cyber Evidence* (Glasser Legal Works 2003) (a looseleaf treatise, periodically supplemented)

Fios, www.fiosinc.com (provider of electronic discovery services – website contains articles, samples forms and archived webcasts; sponsor of Discovery Resources.org)

D.Gourash, et al., *Spoliation of Evidence: Sanctions and Remedies for Destruction of Evidence in Civil Litigation*, 2d ed. (American Bar Association 2006)

Kroll Ontrack, Inc., www.krollontrack.com (provider of electronic evidence services – website contains articles, case summaries and sample forms for electronic discovery, publishes *Case Law & E-Discovery News*, a free monthly newsletter)

M. Lange and K. Nimsger, *Electronic Evidence and Discovery: What Every Lawyer Should Know*, (American Bar Association 2004)

M. Lange, *New FRCP Rules: What Does it Mean for You?* (KrollOntrack, December, 2006), available at www.krollontrack.com/Publications/frcprules.pdf

M. Mack and S. Pattison, *Electronic Evidence Management – From Creation Through Litigation* (Fios, Inc. 2005)

M. Mack and S. Pattison, *The Process of Illumination: The Practical Guide to Electronic Discovery* (Fios, Inc. 2004)

L. Marco and K. Connolly, “Electronic Records: What to Look and Ask For (with Glossary),” *The Practical Litigator* (March 2004)

National Conference of Commissioners on Uniform State Laws, *Uniform Rules Relating to Discovery of Electronically Stored Information* (August 2007), available at www.nccusl.org

S. Nelson, B. Olson and J. Simek, *The Electronic Evidence and Discovery Handbook* (American Bar Association 2006).

G. Paul and B. Nearon, *The Discovery Revolution – E-Discovery Amendments to the Federal Rules of Civil Procedure* (American Bar Ass’n 2005)

P. Rice, *Electronic Evidence: Law and Practice* (American Bar Ass’n 2005)

C. Roberts, “The 2006 Amendments to the Federal Rules of Civil Procedure,” *Law Practice Today* (August 2006), available at <http://tinyurl.com/qbpdg> or www.abanet.org/lpm/lpt/articles/tch/08061.shtml

S. Scheindlin and J. Rabkin, “Electronic Discovery in Federal Litigation: Is Rule 34 up to the Task,” *41 B.C.L. Rev.* 327 (2000)

S. Scheindlin and K. Wangkeo, “Electronic Discovery Sanctions in the Twenty-First Century.” *11 Mich. Telecom. Tech. L. Rev.* 71

The Sedona Conference, www.thesedonaconference.org:

- *Best Practices for the Selection of Electronic Discovery Vendors: Navigating the Vendor Proposal Process* (The Sedona Conference 2005)
- *Best Practices Commentary on Search & Retrieval Methods* (The Sedona Conference 2007)

- *Commentary on Email Management* (The Sedona Conference 2007)
- *Commentary on Legal Holds* (Public Comment Version) (The Sedona Conference 2007)
- *Glossary for E-Discovery and Digital Information Management* (The Sedona Conference 2005)
- *The Sedona Principles Addressing Electronic Document Production, Second Edition* (The Sedona Conference 2005)

Sensei Enterprises, Inc, www.senseient.com. (provider of legal technology, electronic discovery and computer forensics services)

J. Tredennick, ed. “The New Federal Rules on E-Discovery: The First 180 Days, *Law Technology Today* (July 2007)

K. Withers, www.kenwithers.com/ – website maintained by the Director of Judicial Education and Content of the Sedona Conference (formerly an Associate of the Research Division of the Federal Judicial Center with responsibility for research on discovery of electronic evidence in civil litigation)