



Monday, May 22
4:30–6:00 pm

502 Taming the Records Retention Beast *Legal Manager Track*

Patrick Oot
Director of Electronic Discovery & Senior Counsel
Verizon Legal Department

Miriam M. Smolen
Associate General Counsel
Fannie Mae



502: Taming the Records Retention Beast

Patrick Oot

Director of Electronic Discovery & Senior Counsel

Verizon Legal

Miriam Smolen

Associate General Counsel

Fannie Mae

ACC's 4th Annual Corporate Counsel University:
New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront

The in-house bar association.SM



Overview

- Verizon's Litigation Data Case Study (10 min.)
- Verizon's solution for Document Retention and Litigation Preparedness (5 min.)
- Document Retention Overview (15 min.)
- Charlie Counsel's Bad Day (15 min.)
- Questions (10 min.)



Records Retention Perspectives

● Legal

- Recognize the obligations of the litigation process

● Records Management

- Recognize business and regulatory needs

● Information Technology

- Recognize technology needs of retention policy



Why Records Retention?

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



The Jackpot

- \$1.4 Billion
- *Coleman v. Morgan Stanley*
- \$29.3 Million
- *Zubulake v. UBS Warburg LLC*



Failure to institute or follow a consistent and defensible document retention plan at the early stages of litigation can lead to:

- Increased Litigation Costs
- Fines
- Spoliation Charges
- Adverse Inference Instructions
- Default judgment
- Civil Contempt



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

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

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

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



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

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

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

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Computer History 101

"There is no reason anyone would want a computer in their home." -- Ken Olson, president, chairman and founder of Digital Equipment Corp., 1977



Facts and Figures

21,900,000,000,000

Jupiter Research Estimate on the number of e-mails to be sent in 2006

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Facts and Figures at Verizon

1,489,277

Number of collected e-mails in a recent medium-sized matter with 82 custodians
About 972 Gb or Almost 1 Tb of data

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Facts and Figures at Verizon

2,403,299

Total Files collected in a recent medium-sized matter with 82 custodians 1.3 Tb

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Facts and Figures at Verizon

\$7,593,007.95

**Facts and Figures at another Fortune 500 company
(similar matter – same number of custodians)**

\$42,000,000.00

**Cost of Electronic Discovery Charges and Contract Attorney Review
Medium Sized 82 Custodian Matter**

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront

A large, solid black shape that tapers from left to right, positioned above the main title.

Record Retention Goal: Meet Litigation Obligations & Save Money

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Phase I

Build a Team

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Phase II

Know The Process

Company data has a lifecycle and a roadmap during the litigation
process.

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Typical E-Discovery Process



Phase III: Low Hanging Fruit

Create Standards

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Phase IV

Innovate

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Innovation 1

Central Archive

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Save Processing Fees

Litigation Ready Data

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Central Archive

Save \$1,054,352.00

Data processing for a recent medium-sized matter with 82 custodians

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Innovation 3

Search and Retrieval Technology

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Contract Attorney Expenditure

\$4,043,384.21

One recent medium-sized matter with 82 custodians.
Not Including Outside Counsel Management Hours.



Software Evaluation: Comparative Results

Key Metrics overall: Recall and Precision

	Recall	Precision
Product safety Research		
Reviewer	56.3%	86.6%
Software	98.8%	88.3%
Product Modification		
Reviewer	54.0%	88.2%
Software	93.7%	74.8%
Product Marketing		
Reviewer	43.0%	67.4%
Software	94.5%	79.5%



Innovation 4

Integration

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Integration

Automate

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Phase V

Influence Policy

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Policy Initiatives

The Sedona Conference Working Groups
Reasonable Discovery
Judicial Education
Fortune 500 Education Events

ACC's 4th Annual Corporate Counsel University: New Challenges/New Solutions

May 21-23, Baltimore Marriott Waterfront



Records Management Goals

- KEEP records long enough to meet requirements
- LOCATE records when needed
- PROTECT records when needed
- DESTROY records as soon as they have met retention requirements



Key Tasks

- Developing and maintaining an enforced corporate records program
- Establishing and implementing legal “hold” management
- Establishing a protocol for handling electronic records

Companies without proper “hold” capabilities risk criminal and civil exposure if records cannot be located



KEEP RECORDS

- Keep records long enough to meet business and legal requirements throughout company and across media types
- Establish retention lengths
 - Established across company vs. discretion by employee
- Inventory:
 - What type of records and in what form are they kept?
 - Who is the custodian of the records
 - How are records named? Do names reflect ownership?



Inventory of Electronic Records

- Current IT systems
 - Do systems save historical data (i.e. accounting systems)
- Legacy systems
- Current email systems
 - What is delete cycle?
 - Multiple employee addresses?
 - Administrative Assistant as recipient
- Legacy email systems
- Saved Instant Messages
- PDA messages
- Local drives (no back-ups)
- Shared drives
- Removable media (CD etc.)
- Current back-up tapes used in ongoing recycling
 - Weekly, daily, one-time
- Legacy back-up tapes
- Hard drives retained of former employees
- Discussion databases (i.e. Sharepoint sites)



Inventory of non-electronic records

- Paper
 - Official Business records vs. working papers or drafts
 - Located onsite or offsite
 - Standardized names for archival storage
- Voicemail
 - Retention periods vary
 - May be converted to other form



Protect Records

- **Litigation Holds**
 - Judge Scheindlin in *Zubalake* describes spoliation as “the destruction or significant alteration of evidence, or the failure to preserve property for another’s use as evidence in pending or reasonably foreseeable litigation.
 - Morgan Stanley & Co. paying a \$15 million fine and reforming its e-mail retention practices to resolve SEC charges it failed to produce tens of thousands of requested emails.
 - Creative Science Systems, in copyright infringement lawsuit, sanctioned for failing to preserve operating systems on three of forty servers. Sanction was to bear the cost of analyzing the remaining servers.



Litigation Holds

- Duty to preserve evidence is triggered even before litigation is commenced.
 - Need to know where to look for documents before first request comes in
 - Need plan to retrieve records
 - Need plan to document how search and retrieval conducted



Document Destruction Statutes

- **Sarbanes-Oxley Act of 2002**
 - Sec. 802 §1519: Corporate Responsibility for the improper destruction of documents done “knowingly ... with the intent to impede, obstruct or influence ...”
 - Sec. 802 §1102: Criminal sanctions for interfering with official proceedings for intentionally destroying or concealing a record.

- **Other Criminal Liability Statutes regarding Document Destruction**
 - 18 U.S.C. §1503: catch-all provision making it a crime to “corruptly” endeavor to impede or obstruct the “due administration of justice.”
 - 18 U.S.C. §1505: provides for criminal liability for destroying documents demanded under the Antitrust Civil Process Act.
 - 18 U.S.C. §1512(b): provides for criminal liability for obstructing justice by “corruptly persuad[ing] another to destroy documents with the intent to impede an official proceeding.
 - 18 U.S.C. §1519: provides criminal liability for whoever knowingly alters, destroys, mutilates, conceals, covers up, or makes a false entry in any record with the intent to obstruct a federal investigation.



Records Retention Notices

- When need for litigation hold is identified, records retention notice should be send
 - Identify all necessary recipients
 - Document that recipients received and complied with notice
 - Determine who should collect documents
 - Internal Audit/Investigations
 - In-house Counsel
 - Outside Counsel
 - IT department needs to be involved
 - IT liaison should be identified prior to any litigation hold becoming necessary



Retention of Backup Tapes

- Upon litigation hold, need to consider which backup tapes to retain
 - Tape data of key players
 - Wholesale retention = huge cost/storage space
- Proposed new Federal Civil Discovery Rules regarding e-discovery
 - Rule 37: 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.



Destroy Records when Obsolete

- Very few records require permanent retention
 - Records fail to be destroyed because housed in multiple locations
 - Fear of inappropriate destruction
 - Records are under control of central inventory

- Disposal should follow policy. Automate where possible.
- Lack of proper destruction can increase costs in retention, and future document productions
- Ensure that documents no longer subject to litigation holds be destroyed according to retention policy
- Review old records stored off-site to come into compliance with records retention policy



Employee Adherence to Policy

- Records retention policy often low on employees' radar
- Is policy enforced through employee sanctions?
- Vendors need to comply with company policy while performing company services



What area should Charlie Counsel tackle first?

- A. Rewrite the Records Retention Policy to ensure it covers all records with appropriate retention time frames.***
- B. Inventory the types and locations of all records.***
- C. Institute a push to ensure all business units are using the same procedures and naming conventions for saving records.***
- D. Focus on correct retention of emails since those are usually key evidence in the event of a litigation hold.***



Q: What should Charlie Counsel do about old backup tapes?

- A. Ignore them. Charlie's got higher priorities right now.*
- B. Locate all old backup tapes and destroy those outside the retention period.*
- C. Inventory all old backup tapes and save them even if outside the retention period.*
- D. Review the old tapes and only save those that contain the Email servers.*



Q: Based on an internal Hotline complaint, should Charlie Counsel order a litigation hold suspending normal record retention guidelines?

- A. No. There is not sufficient basis to believe that litigation or an investigation is threatened to suspend the guidelines.*
- B. No. It is too costly to suspend the guidelines merely for a Hotline complaint.*
- C. No because Internal Audit does not believe this is a legitimate complaint at this time.*
- D. Yes. The risks of destroying what could be relevant evidence outweigh the costs or the fact that the complaint has not been verified.*



Q: If the Hotline complaint has validity, should Charlie Counsel hire outside counsel at this time to collect documents?

A. No. Charlie can rely on his Internal Audit team to collect relevant documents.

B. No. Charlie should use his in-house counsel to collect documents without Internal Audit.

C. Yes. It is worth the cost of outside counsel to ensure that there can be no criticism of the document collection.

D. No. Charlie should send out a retention memo with instructions to employees, and have them retain their own relevant documents.



Q. If Charlie Counsel had ordered that all records past the retention period be destroyed BEFORE he knew about the SEC investigation, is he ok?

A. No. The government does not care about the legitimacy of following retention policy procedures, just that relevant material was destroyed.

B. Yes. The company's obligation to retain relevant evidence only starts when there is knowledge of a possible investigation.

C. Yes. The government understands that it is too costly for companies to keep all records just for Hotline complaints.

D. Who cares! Charlie should immediately try and get his old job back!

WHITE PAPER

E-Mail Discovery in Civil Litigation:
Worst Case Scenarios vs. Best Practices

Jeffrey Plotkin
Attorney at Law
Eiseman Levine Lehrhaupt
& Kakoyiannis, P.C.
845 Third Avenue
New York, NY 10022

APRIL 2004

© 2004 Eiseman, Levine, Lehrhaupt & Kakoyiannis, P.C. All rights reserved.

Compliments of



now from



TABLE OF CONTENTS

About the Author

INTRODUCTION

I. WHO PAYS FOR E-MAIL DISCOVERY?

A. Disaster Recovery

1. Backup Tapes
2. "Cost-Shifting" of Backup Tape Restoration and Search
3. Avoiding the Backup Tape Dilemma

B. Hard Drive Discovery

1. Decentralized E-Mail
2. "Deleted" E-Mails
3. Avoiding Hard Drive Discovery Problems

II. PRESERVATION OF E-MAIL EVIDENCE

A. Duty to Retain E-Mail

B. Sanctions for "Spoliation" of E-Mail

C. Avoiding Spoliation Claims

D. Additional Considerations

ABOUT THE AUTHOR

Jeffrey Plotkin is a Partner in the Litigation Department of the New York City law firm of Eiseman, Levine, Lehrhaupt & Kakoyiannis, P.C. He formerly served as Assistant Regional Administrator of the Securities and Exchange Commission's New York Regional Office, in the Division of Broker-Dealer Enforcement.

Mr. Plotkin is a consultant for KVS, Inc., a leading provider of e-mail archiving and management software. He has authored other White Papers respecting legal issues surrounding e-mail, including "Coping with Broker-Dealer Regulations Concerning E-Mail," and "Corporate Governance – The Impact on Your IT Department," both available through www.kvsinc.com. Mr. Plotkin has been quoted in the Wall Street Journal, Investment News, and Wall Street & Technology, with respect to regulatory issues involving e-mail.

For further information concerning Mr. Plotkin, please visit www.SECDefense.com.

INTRODUCTION

This White Paper addresses the complications that regularly arise during discovery in civil litigation as a result of a corporate defendant's faulty or insufficient systems and procedures for e-mail retention and management. These complications, all of which are avoidable, increase litigation costs so exponentially that, in many cases, settlement becomes the only viable option.

The e-mail discovery issues addressed herein fall into two broad categories. The first category concerns "cost-shifting," particularly: (1) which party should pay the extraordinary costs associated with retrieval of e-mails from disaster recovery backup tapes; and (2) which party should pay the substantial costs associated with hard drive discovery for (a) e-mails stored in a decentralized, non-network environment (*e.g.*, where responsive e-mails are dispersed among the hard drives of individual users); and (b) e-mails that have been "deleted" from mailboxes and now reside as on the hard drive as "residual" data?

The second category concerns retention of e-mails, particularly: (1) what duty does a party generally have to preserve e-mails prior to and during litigation; and (2) what sanctions are appropriate against a party who fails in that duty?

I.

WHO PAYS FOR E-MAIL DISCOVERY?

A. Disaster Recovery

1. Backup Tapes

Historically, as a disaster recovery mechanism, companies have utilized commercially available software to take a periodic "snapshot" of the data on the company's servers, including e-mail files. That data is stored on magnetic tape, which is commercially available

in various formats. Vast amounts of data can be stored on a single magnetic tape. If a catastrophic event occurs, the data previously captured on magnetic tape from the last backup period can be reloaded to allow the company's computer systems to startup again with minimal loss.

Back-up tapes . . . are not archives from which documents may easily be retrieved. The data on a backup tape are not organized for retrieval of individual documents or files, but for wholesale, emergency uploading onto a computer system. There, the organization of the data mirrors the computer's structure, not the human records management structure if there is one.

Rowe Entertainment, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421 (S.D.N.Y. 2002) (citation omitted).

Companies utilize different disaster backup protocols. A typical backup protocol provides for creation of back up tapes at three intervals: end of each business day; end of each business week; and end of each business month.¹ Nightly backup tapes may be kept until the end of the week or month, weekly tapes may be kept until the end of the month or year, and monthly tapes may be kept until the end of the year or for a number of years. After the expiration of the retention period for each backup tape, the tapes are recycled and overwritten.

Periodic backups necessarily entail the loss of certain e-mail. If employees delete e-mails from the server prior to the expiration of a given backup period, that e-mail would not appear in the following periodic snapshot of the e-mail files. For instance, if an employee deleted an entry from his e-mail box prior to the end of the month, that entry would not be captured on the monthly back-up tapes (but might appear on the daily or weekly backup tapes, if they still exist). On the other hand, unless a user deletes e-mails between backups, each

¹ See, e.g., *Wiginton v. Ellis*, 2003 WL 22439865 at *2 (N.D. Ill. Oct. 27, 2003). Some companies also employ incremental backups, *i.e.*, a backup of files that have changed since the last backup.

backup tape may contain duplicate e-mails, *i.e.*, e-mails that were captured on previous backup tapes.

It is a sound business practice to utilize magnetic backup tapes as a disaster recovery mechanism. However, litigation complications arise when the backup tapes are the only place where an opposing party can discover relevant e-mails.² In order to access e-mail on a disaster recovery backup tape, the data has to be “restored.”

Restoration of e-mails from backup tapes is a lengthy and expensive process. Among other things, the company must first locate and catalog the tapes that may contain the relevant mailbox files. During the restoration process, the company must clean and check the functionality of the tape drive regularly, because backup tapes physically get dirty or dusty from years of storage.³ Once the data is accessed,⁴ the company must determine which directories on the backup tape need to be restored. The company then must clear sufficient disk space on a hard drive, because each backup tape represents a snapshot of the server’s hard drive on a given date, and each date must be restored separately on to a hard drive.⁵ The company then restores the responsive data onto a hard drive.

² A company’s duty to preserve backup tapes, once it has notice of a potential or actual litigation, is discussed in Section II below.

³ Successful restoration of back-up tapes cannot be guaranteed in any individual instance, because the tapes may have been corrupted during storage (*e.g.*, moisture corruption). And the attempts to restore the back-up tapes may corrupt them even further.

⁴ Because of advances in technology, a company may no longer currently utilize the tape format that it utilized to backup the data years before. As a result, the company may no longer have the hardware necessary to access and utilize a particular tape format, or it may no longer maintain the software it previously utilized to create the backup.

⁵ In *Concord Boat Corp. v. Brunswick Corp.*, 1997 WL 33352759 at *8 – 9 (E.D. Ark. Aug. 29, 1997), defendant’s information systems support manager informed the court that “restoring a backup copy of the . . . e-mail system onto . . . [the] Host Server would destroy the current version of the . . . e-mail system and jeopardize [the company’s] continuing data processing activities. It would therefore be necessary to duplicate [the company’s] computing environment as it existed at the time the back up tape was created on a separate computer system.”

Once restoration of the data is accomplished, commercially available software could be used to extract a particular individual's e-mail file. For instance, the e-mail file can be exported onto a Microsoft Outlook data file, which in turn can be opened in Microsoft Outlook, a common e-mail viewer application. A user could then browse through the mail file and sort the mail by recipient, date or subject, or search for key words in the body of the e-mail. Also, software may be used to "de-duplicate" the e-mail files, *i.e.*, remove duplicate copies of e-mails.

Complications regularly arise during the restoration process. E-mail attachments in formats that cannot be searched electronically, such as pdf. files (scanned image files), must be converted into text-searchable files.⁶ Further, the passwords for protected e-mails and attachment files must be "broken." And in many instances where the e-mail files cannot be exported successfully to commercially available software, companies must develop a software script to run the requested search phrases through the restored data.

The estimated and actual costs for restoring backup tapes and searching restored e-mails vary widely, depending on whom you talk to. However, in most large cases, the costs are extraordinary. *See Medtronic Sofamore Danek, Inc. v. Michelson*, 2003 WL 21468573 at * 11 (W.D. Tenn. May 13, 2003) (consultant charged a total of \$605,000 to restore, search, and de-duplicate 124 sample backup tapes, or \$4,881 per tape); *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280, 282-83 (S.D.N.Y. 2003) (consultant charged an average of \$2,304.92 per backup tape to restore and text-search e-mails).

⁶ Where a company wishes to print-out hard copies of all restored e-mails and attachments, and search the documents manually rather than electronically for responsiveness and privilege, ease of mass printout may be facilitated by converting all e-mails and attachments to a TIFF (Tagged Image File Format). *See, e.g., Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, 2002 WL 246439 at *2 (E.D. La. Feb. 19, 2002).

2. “Cost-Shifting” of Backup Tape Restoration and Search

Historically, the party responding to a discovery request bears the costs of producing responsive and relevant materials in its possession, custody, and control. However, the responding party “may invoke the district court’s discretion under [Federal Civil Procedure] Rule 26(c)⁷ to grant orders protecting him from ‘undue burden or expense’ in doing so, including orders conditioning discovery on the requesting party’s payment of the costs of discovery.” *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 358, 98 S. Ct. 2380, 2393 (1978).

In the past, in the realm of paper-based discovery, it was the rare case where a defendant requested that the court shift the costs of discovery to the plaintiff, and the even rarer case where the court granted such request. However, in the current realm of electronic discovery, defendants increasingly are asking the courts to shift some or all of the costs of electronic discovery, particularly backup tape restoration, to the requesting party.

The courts are mindful that their ultimate decision on this issue may represent the defining moment in the litigation. As one court noted:

If the likelihood of finding something was the only criterion, there is a risk that someone will have to spend hundreds of thousands of dollars to produce a single e-mail. That is an awfully expensive needle to justify searching a haystack. It must be recalled that ordering the producing party to restore backup tapes upon a showing of likelihood that they will contain relevant information in every case gives the plaintiff a gigantic club with which to beat his opponent into settlement. No corporate president in her right mind would fail to settle a lawsuit for \$100,000 if the restoration of backup tapes would cost \$300,000. While that scenario might warm the cockles of certain lawyers’ hearts, no one would accuse it of being just.

McPeck v. Ashcroft, 202 F.R.D. 31, 34 (D.D.C. 2001).

⁷ Pursuant to FRCP 26(c), a court may enter “any order which justice requires to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including . . . (2) that the . . . discovery may be had only on specified terms and conditions”. The civil procedure rules of the various states have similar provisions.

An instructive case that will be discussed at length here is *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) (“*Zubulake I*”), not only because it articulates a currently accepted standard for cost-shifting in backup tape cases, but also because it minutely details the aggravations, burdens and costs attendant to producing e-mails from backup tapes.

UBS, a broker-dealer registered with the SEC, backed up its e-mails in two ways, on magnetic backup tapes or on optical disks.⁸ In response to *Zubulake*’s broad e-mail discovery request, UBS preliminarily determined that responsive e-mail files were contained on a total of 94 backup tapes. Before UBS undertook the task of restoring and searching the backup tapes for responsive e-mails, it petitioned the court to shift the cost of production to *Zubulake* to protect it from undue burden or expense, pursuant to FRCP 26(c).

The *Zubulake* court stated that it first had to ascertain whether the data was kept in an “accessible” or “inaccessible” format in order to determine whether production of electronic data was unduly burdensome or expensive under FRCP 26(c). The court listed five categories of electronic data, from most accessible to least accessible -- the second least accessible being “backup tapes.”

The court stated:

The disadvantage of tape drives is that they are sequential-access devices, which means that to read any particular block of data, you need to read all the preceding blocks. As a result, the data on a backup tape are not organized for retrieval of individual documents or files because the organization of the data mirrors the computer’s structure, not the human records management structure. Backup tapes also typically employ some sort of data compression, permitting more data to be stored on each tape, but also making restoration more time-consuming and expensive, especially given the lack of uniform standard governing data compression.

Id. at 319 (quotations marks, brackets, ellipses, footnotes and citations omitted).

⁸ In particular, UBS stored on optical disk outgoing and incoming external e-mail to and from registered traders. Internal e-mails, however, were not stored on this system. Because the optical disks were easily searchable using publicly available software, the court ordered UBS to search all optical disks at its cost.

Because it found that the UBS backup tapes were “inaccessible,” the court ruled it was appropriate to consider cost-shifting. Using as its starting point a “balancing approach” articulated by courts in other e-discovery disputes (primarily the eight-factor test articulated by *Rowe*), the court fashioned a cost-shifting test with seven factors, in the following descending order of importance:

1. The extent to which the request is specially tailored to discovery relevant information;
2. The availability of such information from other sources;
3. The total cost of production, compared to the amount in controversy;
4. The total cost of production, compared to the resources available to each party;
5. The relative ability of each party to control costs and its incentive to do so;
6. The importance of the issues at stake in the litigation; and
7. The relative benefits to the parties of obtaining the information.

Id. at 321-22.

Given the uncertainty of whether the backup tapes would yield probative evidence, the court ordered UBS, at its own cost, to restore and produce responsive e-mails from a sample of five backup tapes selected by Zubulake. The court ordered that UBS submit an affidavit detailing the results of its search of the five sample backup tapes, as well as the time and money spent on the search. After further review, the court would issue a final ruling on the cost-shifting issue, based on the tangible evidence the tapes offered, and the tangible evidence of the time and cost required to restore the backup tapes.⁹ *See Id.* at 323-24.

⁹ This protocol (*i.e.*, initial sampling results followed by a final decision on cost-shifting) has been utilized in numerous other backup tape cases. *See, e.g., McPeck*, 202 F.R.D. at 34-35; *Linnen v. A.H. Robbins Co., Inc.*, 1999 WL 462015 at *6 (Mass. Super. June 16, 1999).

Pursuant to the court's order, UBS restored and produced e-mails from the five backup tapes. *See Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003) ("*Zubulake II*"). After reviewing the results, Zubulake moved for an order compelling UBS to produce all remaining e-mails at its expense. UBS, which had revised the number of remaining backup tapes to be seventy-seven, continued to argue that the costs should be shifted entirely to Zubulake.

UBS reported to the court that it used an outside vendor to perform the restoration of the backup tapes. The consultant restored each of the tapes, yielding a total of 6,203 unique (non-duplicated) e-mails. The consultant then performed a search for e-mails containing relevant text or header terms (such as "Zubulake"), and found 1,541 responsive e-mails. UBS deemed 600 of the e-mails to be relevant and produced them.

The consultant billed UBS a total of \$11,524.63 (\$2,304.92 per tape). In addition, UBS incurred \$4,633 in attorney fees for the document review, and \$2,845 in paralegal fees for tasks related to document production. UBS also paid \$432.60 in photocopying costs (reimbursed by Zubulake). The total cost of restoration and production from the five backup tapes was \$19,003.43 -- almost four thousand dollars per tape. *See Id.* at 283.

UBS asked the court to shift the cost of further production, estimated to be \$273,649 (\$165,954 to restore and search the tapes, and \$107,694 for attorney and paralegal review costs), to Zubulake.

Upon review of the search results from the five backup tapes, the court found that 68 of the 600 e-mails presented by Zubulake to the court were relevant to the case. After applying the seven part test to the facts and circumstances of the case, the court ordered that UBS bear 75% of the estimated \$165,000 cost of restoring and searching the remaining

backup tapes, and 100% of the estimated \$107,000 cost of reviewing and producing the electronic data once it has been converted to an accessible form. In other words, the court ordered UBS to incur an additional \$240,000 to restore and search the remaining e-mails. This number, of course, did not include the legal fees and costs incurred in litigating the issue twice before the court. *See Id.* at 284-91.

Other defendants in other cases have fared better or worse in shifting some of the costs of backup tape restoration to the plaintiffs. In *Medtronic*, the court ordered defendant to bear 60% of the total estimated cost of \$605,300 to restore, search, and de-duplicate e-mails from 124 sample backup tapes. That cost excluded attorney privilege review, and production costs. *See Medtronic*, 2003 WL 21468673 at *11.

In *Byers v. Illinois State Police*, 2002 WL 1264004 (N.D. Ill. June 3, 2002), even though the court found it highly unlikely that a search of backup tapes would yield relevant e-mails, the court ordered the defendant to bear 100% of the expense of restoring and searching daily backup tapes for an eight year period. However, because the defendant recently had converted to a new e-mail program that could not read the e-mails contained on the backup tapes, the court shifted the costs to plaintiff to license the old e-mail program at a cost of \$8,000 month.

Because of cases like *Zubulake*, a move is afoot to amend the Federal Rules of Civil Procedure to codify cost-shifting standards in e-discovery cases. The Civil Rules Advisory Committee of the U.S. Judicial Conference currently is considering whether to propose amendments to F.R.C.P. Rule 26 addressing electronically stored data. The Committee's most-current draft of a proposed Rule 26(h)(2), with its variable alternatives, shows the inherent difficulties of framing an ironclad rule regarding cost-shifting:

Inaccessible electronically-stored data. In responding to discovery requests, a party need not include electronically-stored data [from systems] created only for disaster-recovery purposes, [providing that the party preserves a single day's full set of such backup data,] or electronically-stored data that are (not [reasonably] accessible without undue burden or expense) [accessible only if restored or migrated to accessible media and format] (not accessible [reasonably available] in the usual course of the responding party's (business) [activities]). For good cause, the court may order a party to produce inaccessible electronically-stored data subject to the limitations or Rule 26(b)(2)(B), [and may require the requesting part to bear some of all of the reasonable costs of (any extraordinary efforts necessary in) obtaining such information.

Rick Marcus, *Memorandum to Advisory Committee on Civil Rules re: E-discovery rule discussion proposals* at 19-20 (Sept. 15, 2003).

3. Avoiding the Backup Tape Dilemma

UBS's dilemma in *Zubulake* was easily avoidable. UBS should have archived all its e-mails on accessible and easily searchable storage media, separately from, and in addition to, its disaster recovery backup tapes. UBS, through commercially available software, easily could have automatically journaled all its employees' e-mails to a central data store, from which archived copies of the e-mails could be created on optical disk, CD-ROM, or optical tape.¹⁰

Indeed, UBS, an SEC registered broker-dealer, was required to archive all its e-mails for three years in a non-erasable, non-alterable format, as proscribed by SEC Exchange Act

¹⁰ *Accord The Sedona Principles -- Best Practices Recommendation & Principles for Addressing Electronic Document Production* at 23 (The Sedona Conference, March 2003) ("Organizations seeking to preserve data for business purposes or litigation should, if possible, employ means other than disaster recovery backup tapes. Alternatives include utilizing copies of relevant files, "snap" server copies, and targeted archive tape creation.").

Rule 17a-4(f).¹¹ If UBS simply had followed that rule, and had stored e-mails correctly, it would have saved hundreds of thousands of dollars of discovery costs and legal fees.

B. Hard Drive Discovery

1. Decentralized E-Mail

Another e-discovery issue that regularly arises is where the company's e-mail is not centrally stored and managed on the firm's network server. For instance, it is often the case that the only copies of responsive e-mails are located on the individual hard drives of multiple employees' personal computers or laptops. Discovery under these circumstances can get especially complicated where the individual employees' computers use a variety of different e-mail programs, so that all files cannot be reviewed by a single search program.¹²

During litigation, some companies with decentralized e-mail storage issues have attempted to shift the costs of e-discovery to the other party, with mixed results. In *Medtronic*, the court refused to shift costs, and ordered the defendant, at its own cost, to search through 300 gigabytes of individual user e-mails, using Boolean search terms provided by plaintiff's counsel. *See Medtronic*, 2003 WL 21468573 at *9.

¹¹ *See generally*, Jeffrey Plotkin, *Broker-Dealer Regulations Concerning E-Mail*, New York Law Journal, December 4, 2002. At the time the SEC's rule was promulgated, the industry standard for non-alterable, non-erasable electronic storage media was "WORM" ("write once, read many") storage on optical disk, optical tape, and CD-ROM. With WORM, digital information is permanently "burned" onto the hardware, and consequently, the information could not easily be altered or deleted. In May 2003, the SEC issued a release allowing broker-dealers to employ electronic storage systems that prevent records from being rewritten or erased without relying solely on the system's hardware features. *See* SEC Release No. 34-47806 (May 12, 2003). In particular, the SEC approved the use of a new storage technology that utilizes integrated hardware and software codes intrinsic to the system to prevent overwriting, erasure, or alteration of digitally stored records. The system stores an expiry or retention period with each record or file system. The system described in the SEC release is EMC's Centera. According to EMC, compared to standard WORM storage, Centera users can expect a reduction in their overall storage capacity requirement by 50%.

¹² In order to conduct a decentralized search of individual user's hard drives, a company may hire a consultant to obtain a "mirror image" of the hard drives containing e-mails, and formulate and implement a search procedure. *See Rowe*, 205 F.R.D. at 433.

In *In re Amsted Industries, Inc. "ERISA" Litigation*, 2002 WL 31844956 (N.D. Ill. Dec. 18, 2002), defendants chose not to conduct an actual hard drive search of individual user e-mails, but instead "investigated" whether responsive e-mails existed by "questioning individuals regarding e-mails on their computers." The plaintiffs argued that this investigation was inadequate and that the defendants were required to actually search the hard drive of each individual defendant and each person having access to relevant information to determine whether there is discoverable material.

The court agreed, and ruled that defendants "should also search the in-box, saved, and sent folders of any relevant individual's e-mail in the same manner. We recognize that Amsted's retention policy and its lack of a comprehensive e-mail system . . . make it unlikely that the additional searches are going to turn up relevant discovery. On the other hand, [the requested search is not] so burdensome or expensive as to require a limiting of the requests." *Id.* at *2.

2. **"Deleted" E-Mails**

Many e-mail users still linger under the impression that once they delete an e-mail from their mailbox, it is gone forever. This simply is not the case.

"Deleting" a file does not actually erase that data from the computer's storage devices. Rather, it simply finds the data's entry in the disk directory and changes it to a "not used" status – thus permitting the computer to write over the "deleted" data. Until the computer writes over the "deleted" data, however, it may be recovered by searching the disk itself rather than the disk's directory. Accordingly, many files are recoverable long after they have been deleted – even if neither the computer user nor the computer itself is aware of their existence. Such data is referred to as "residual data."

Zubulake, 217 F.R.D. at 313 n. 19, quoting Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. Rev. 327, 337 (2000) (footnotes omitted).¹³

Under normal circumstances, a party responding to an e-mail discovery request has no obligation to attempt to restore e-mails deleted in the ordinary course of business.¹⁴ However, plaintiffs routinely demand that corporate defendants allow them to inspect the defendants' computer systems to discover deleted e-mails that may still exist on hard drives. The courts have been amenable to ordering such discovery (including inspection not only of the company's network servers, but also of individual employees' personal computers and laptops), usually at the plaintiff's cost, where there is evidence that responsive e-mails may have been deleted.

Aside from the occasional practice of "dumpster diving," the discovery of deleted computer documents does not have a close analogy in conventional, paper-based discovery. Just as a party would not be required to sort through its trash to resurrect discarded paper documents, so it should not be obligated to pay the cost of retrieving deleted e-mails. Thus, since there has been no showing that the defendants access . . . their deleted e-mails in the normal course of business, this factor[] tips in favor of shifting the costs of discovery to the plaintiffs.

Rowe, 205 F.R.D. at 431 (quotations marks, citation and footnote deleted).

A standard protocol has emerged from the courts in cases where the plaintiff demands inspection of the defendant's computers to search for deleted e-mails. A computer expert,

¹³ "Deleted data may also exist because it was backed up before it was deleted. Thus, it may reside on backup tapes or similar data." *Id.*

¹⁴ *But compare* ABA Litigation Task Force on Electronic Discovery, Standard 29(a)(iii) (Aug. 1999) ("Unless a requesting party can demonstrate a substantial need for it, a party does not ordinarily have a duty to take steps to try to restore electronic information that has been deleted or discarded in the regular course of business but may not have been completely erased from computer memory"), with ABA Litigation Task Force on Electronic Discovery, November 2003 Draft Amendments to Electronic Discovery Standards, Standard 29(a)(iii) (Nov. 17, 2003) ("Electronic data as to which a duty to preserve may exist include data that have been deleted but can be restored"), both available at [http://www.fjc.gov/public/pdf.nsf/lookup/ElecDi12.pdf/\\$file/ElecDi12.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/ElecDi12.pdf/$file/ElecDi12.pdf)

either selected by the plaintiff or acceptable to both parties, is appointed by the court to create a “mirror image” of the hard drive. The plaintiff pays the expert’s fees and expenses, and the defendant makes its computers and its technical personnel available to the computer expert. After the expert completes his technical tasks, he provides to the defendant’s counsel all recovered e-mails (or in some cases, provides the data to plaintiff’s counsel for “attorneys’-eyes-only” review). Defendant’s counsel then reviews the records for privilege and responsiveness, at defendant’s expense, and makes production to plaintiff.¹⁵

Even though the courts typically order the plaintiffs to shoulder the costs of the expert inspection and search for deleted e-mails files, the inspection process itself creates disruption of and interference with defendant’s business. Additionally, if the plaintiff does not voluntarily agree to pay the costs associated with deleted e-mail restoration, defendants must then expend significant legal fees in motion practice to resist plaintiff’s attempts to impose the costs of e-mail restoration on the defendant.

And finally, as discussed at length in Section II below, if a plaintiff learns through a hard drive inspection of the computer’s computers that the company’s employees have deleted responsive e-mails from hard drives in violation of an obligation to preserve relevant evidence, such plaintiff will seek, and may well obtain, significant sanctions against the company for “spoliating” evidence.

3. Avoiding Hard Drive Discovery Problems

The hassles and costs of litigating over hard drive searches and inspections may be easily avoided by basic e-mail management tools and procedures. Most importantly, a

¹⁵ See, e.g., *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 652-54 (D. Minn. 2002); *Rowe*, 205 F.R.D. at 433; *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 641-44 (S.D. Ind. 2000); *Playboy Enterprises v. Welles*, 60 F. Supp.2d 1050 (S.D. Cal. 1999).

company's policy should mandate, and the company's technology should allow, that all employee e-mails (including, if plausible, instant messages, and e-mails from employees' laptops, cell phones, PDAs, and home computers)¹⁶ be sent, received, captured, or routed, on a central server or servers, and thereafter archived on easily accessible and searchable storage media.

As such, if an employee deletes e-mail from his mailbox, original copies of that e-mail still will reside in the firm's archived records, and not just possibly on backup tapes. No need will exist for a plaintiff to request access to any individual employees' hard drives during civil discovery, and no reasonable ground will exist for plaintiff to accuse the defendant or its employees of deleting responsive e-mail.

The costs of responding to discovery of information contained in computer systems can be best controlled if the organization takes steps ahead of time to prepare computer system and users of these systems, for the potential demands of litigation. Such steps include institutionally defined, orderly procedures for preserving and producing relevant documents and data, and establishing processes to collect, store, review, and produce data that may be responsive to discovery requests or required for initial mandatory disclosures. Preparation for electronic discovery can also help the corporation accurately present the cost and burden of specific discovery requests to the court, control the costs of reasonable steps to produce data, and avoid the risk of failing to preserve or produce evidence from computer systems.

The Sedona Principles at 19.

II.

PRESERVATION OF E-MAIL EVIDENCE

A. Duty To Retain E-Mail

A company has an obligation to preserve potentially relevant electronic records in its possession or control in connection with an anticipated litigation or commenced litigation.

¹⁶ If it not feasible to route or capture on the firm's server employee e-mails that were sent or received outside of the firm's server environment, a company should consider prohibiting or limiting such extra-network e-mail altogether.

“The obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.” *Zubulake v. UBS Warburg LLC*, 2003 WL 22410619 at *2 (S.D.N.Y. Oct. 22, 2003) (*Zubulake IV*) (citations omitted).

A party’s obligation to preserve evidence that may be relevant to litigation is triggered once the party has notice that litigation might occur. *See, e.g., Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998). The obligation to preserve electronic evidence exists independent of any preservation order of the court, preservation demand from the opposing party,¹⁷ or discovery demand from the opposing party. *See e.g., Danis v. USN Comm., Inc.*, 2000 WL 1694325 at *1, 32-33 (N.D. Ill. Oct. 23, 2000); *Proctor & Gamble Co. v. Haugen*, 179 F.R.D. 622, 631 (D. Utah 1998), *aff’d in part, rev’d in part on other grounds*, 222 F.3d 1262 (10th Cir. 2000).

The duty to preserve electronic evidence must be discharged actively. Senior management must advise employees in possession of discoverable materials of their obligations to preserve documents known to be relevant to the issues in the litigation, or reasonably calculated to lead to the discovery of admissible evidence, or reasonably likely to be requested during discovery, or known to the subject of a pending discovery demand. If the court has entered a preservation order in the case, senior management must provide employees with a copy of the court’s order and acquaint them with the potential sanctions that could issue for non-compliance with the order. The company also should implement and distribute to employees a comprehensive written preservation plan with specific criteria for finding and securing relevant electronic evidence for the litigation. The company also must

¹⁷ For an example of an electronic evidence preservation demand, *see Wiginton*, 2003 WL 22439865 at *1.

actively monitor compliance with the preservation plan. *See generally Danis*, 2000 WL 1694325 at *32, 37.¹⁸

Zubulake IV sets forth a broad and clear standard for preservation of e-mail on hard drives and backup tapes:

A party or anticipated party must retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any relevant documents created thereafter. In recognition of the fact that there are many ways to manage electronic data, litigants are free to choose how this task is accomplished. For example, a litigant could choose to retain all then-existing backup tapes for the relevant personnel if such tapes store data by individual or the contents can be identified in good faith and through reasonable effort, and to catalog any later-created documents in a separate electronic file. That, along with a mirror-image of the computer system taken at the time the duty to preserve attaches (to preserve documents in the state they existed at that time), creates a complete set of relevant documents. Presumably there are a multitude of other ways to achieve the same result.

....

The scope of a party's preservation obligation can be described as follows: Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents.¹⁹ As a general rule, that litigation hold does not apply to inaccessible backup tapes (*e.g.*, those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if backup tapes are accessible (*i.e.*, actively used for information retrieval), then such tapes *would* likely be subject to the litigation hold.

However, it does make sense to create one exception to this general rule. If a company can identify where particular employees documents are stored on backup tapes, then the tapes storing the documents of "key players" to the existing or

¹⁸ If the company is a public company, it also should instruct outside directors to preserve relevant documents. *See In re Triton Energy Ltd. Securities Litigation*, 2002 WL 32114464 (E.D. Tex. March 7, 2002); *Danis*, 2000 WL 1694325 at *41.

¹⁹ "Whether a company's duty to preserve extends to backup tapes has been a gray area. As a result, it is not terribly surprising that a company would think that it did *not* have a duty to preserve all of its backup tapes, even when it reasonably anticipated the onset of litigation . . . Litigants are now on notice, at least in this Court, that backup tapes that can be identified as storing information created by or for the 'key players' must be preserved." *Zubulake IV*, 2003 WL 22410619 at *6 and n.47 (emphasis in original).

threatened litigation should be preserved if the information contained on those tapes is not otherwise available. This exception applies to *all* backup tapes.²⁰

Zubulake IV, 2003 WL 22410619 at *4 (emphasis in original).

The Advisory Committee on Civil Rules presently is considering proposing an amendment to the Federal Rules of Civil Procedure to address a party's duties to preserve electronic evidence. For instance, draft Rule 26(h)(3) provides:

Preserving electronically-stored data. Upon commencement of an action, the parties must preserve electronically-stored data that may be required to be produced pursuant to Rule [26(a)(1) and] (b)(1), except that materials described by Rule 26(h)(2) need not be preserved unless so ordered by the court for good cause. Nothing in these rules requires a party to suspend or alter the operation in good faith of disaster recovery or other [computer] systems (for electronically –stored data) unless the court so orders for good cause, [providing that the party preserved a single day's full set of such backup data].²¹

B. Sanctions for “Spoliation” of E-Mail

Once a party suspects that the other party or its employees have destroyed or otherwise failed to preserve certain e-mail for discovery, it will petition the court to sanction the opposing party for so-called “spoliation” (*i.e.*, destruction) of evidence.

A court has the inherent and statutory powers to impose sanctions against a party for destroying relevant electronic evidence. *See generally Trigon Ins. Co. v. United States*, 204 F.R.D. 277, 284-85 (E.D. Va. 2001). A court is given broad discretion to choose the appropriate sanction for spoliation given the unique factual circumstances of every case. *See generally Id.* at 287-88.

²⁰ *See also Wiginton*, 2003 WL 22439865 at *7 (the court found that defendant acted in “bad faith” by failing to halt routine recycling of backup tapes, because plaintiff had submitted a preservation letter to defendant requesting that it preserve all backup tapes containing relevant e-mails); *Limmen*, 1999 WL 462015 at *8-11 (defendant violated the court's preservation order by failing to suspend the customary recycling of backup tapes for the electronic mail system. Also, after the court's preservation order was vacated, and after being served with a request for documents that reasonably encompassed backup tapes, defendant violated its general duties to preserve documents by failing to suspend recycling of the backup tapes).

²¹ The draft rule is referring to a “snapshot” backup tape or tapes of all data on the computer system on the day the defendant becomes aware of the suit.

Sanctions for spoliation typically include one or more of the following: (1) default judgment against the defendant, or conversely, dismissal of plaintiff's action;²² (2) an "adverse inference instruction" to the jury;²³ (3) additional discovery at responding party's cost;²⁴ (4) monetary sanctions;²⁵ and (5) attorneys' fees.²⁶

²² This harsh sanction "should only be employed in extreme situations where there is evidence of willfulness, bad faith or fault by the noncomplying party." *Wiginton*, 2003 WL 22439865 at *6 (quotation marks and citation omitted). See *Kucala Enterprises, Ltd. v. Auto Wax Co., Inc.*, 2003 WL 21230605 at *8 (N.D. Ill. May 27, 2003) (dismissal of suit entered against plaintiff company that used a computer program called "Evidence Eliminator" to delete 12,000 files from its owner's desktop computer a few hours before the defendant's computer specialist inspected the computer pursuant to court order), *report and recommendation adopted as modified*, 2003 WL 22433095 (N.D. Ill. Oct. 27, 2003); *Essex Group v. Express Wire Servs.*, 578 S.E.2d 705 (N.C. App. Apr. 15, 2003) (default judgment entered after finding that defendant, *inter alia*, intentionally deleted e-mails); *Nartron Corp. v. General Motors Corp.*, 2003 WL 1985261 at *2-5 (Mich. App. Apr. 29, 2003) (dismissal of plaintiff's complaint for, *inter alia*, intentional destruction of computer records), *appeal denied*, 670 N.W.2d 219 (2003).

²³ Such an instruction directs the jury that it can infer from the fact that defendant destroyed certain evidence that such evidence, if available, would have been favorable to the plaintiff and harmful to the defendant. See, e.g., *3M v. Pribyl*, 259 F.3d 587, 606 n. 5 (7th Cir. 2001) (affirming negative inference instruction where defendant downloaded six gigabytes of music onto his hard drive, overwriting files responsive to plaintiff's demands, on the evening before the computer was turned over for inspection); *Trigon*, 204 F.R.D. at 29 (adverse inference would be drawn respecting the substantive testimony and credibility of the defendant's experts based on their purposeful destruction of e-mails and draft reports).

²⁴ In *Renda Marine, Inc. v. United States*, 58 Fed. Cl. 57 (Fed. Cl. 2003), a contracting officer for the U.S. Government, after receiving notice of a potential litigation claim by a contractor on one of his projects, continued his regular practice of deleting e-mails concerning the project after sending or responding to them. The court ordered that the government produce at its own expense any back-up tapes created on or after the date of notice of the litigation that might contain the deleted e-mails, and granted the plaintiff access to the officer's hard drive to attempt to recover the deleted e-mails. See *Id.* at 62.

²⁵ See, e.g., *Proctor & Gamble Co.*, 179 F.R.D. at 632 (defendant sanctioned \$10,000 for failing to search and preserve the e-mails of five key employees after the litigation was commenced); *Danis*, 2000 WL 1694325 at *53 (CEO of bankrupt defendant corporation sanctioned \$10,000 for failing to implement a suitable document preservation program, thereby leading to the destruction of potentially relevant computerized records).

²⁶ *Landmark Legal Foundation v. E.P.A.*, 272 F. Supp.2d 70, 87 (D.D.C. 2003) (court ordered defendant to pay plaintiff's legal fees and costs in bringing spoliation motion where defendant violated preliminary court order to preserve documents by reformatting the hard drives of several EPA officials, erasing e-mail backup tapes, and deleting e-mails received after date of order); *Kucala Enterprises, Ltd.*, 2003 WL 21230605 at *8 (award of attorneys' fees and costs incurred from time opposing party first willfully deleted computer files to date of hearing on the spoliation motion); *Trigon*, 204 F.R.D. at 291 (award of attorneys fees and costs incurred as a consequence of spoliation of defendant's expert witness e-mails and draft reports); *Linnen*, 1999 WL 462015 at *13 (award of all fees and costs associated with electronic discovery issues arising from improper recycling of backup tapes during litigation).

Differing circuits have differing requirements for establishing spoliation. As discussed in *Zubulake IV*, in the Second Circuit, a party seeking sanctions based on spoliation of evidence must establish three elements:

(1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a “culpable state of mind” and (3) that the destroyed evidence was “relevant to the party’s claim or defense such that a reasonable trier of fact could not find that it would support that claim or defense. . . . [A] “culpable state of mind” for purposes of a spoliation [sanction] includes ordinary negligence. When evidence is destroyed in bad faith (*i.e.*, intentionally or willfully), that fact alone is sufficient to demonstrate relevance. By contrast, when the destruction is negligent, relevance must be proven by the party seeking the sanctions.

Zubulake IV, 2003 WL 22410619 at *6.²⁷

Spoliation motions generally take on a life of their own, and in many cases completely subsume the underlying litigation. See *Danis*, 2000 WL 1694325 at * 50 (“By the parties’ calculations, they have spent an enormous sum of money litigating the sanctions issue: a collective total of \$1,524,762.03. That expenditure has been used solely for the purpose of ‘litigating the litigation,’ and has not contributed to advancing this case to the disposition on the merits that the parties in this case deserve.”).

C. Avoiding Spoliation Claims

To avoid the possibility of spoliation sanctions, and the significant legal fees and costs associated with a spoliation motion, a company must have and follow detailed written procedures concerning evidence preservation.

²⁷ Courts in other circuits utilize slightly different elements in determining whether to grant a spoliation motion. See, e.g., *Applied Telematics, Inc. v. Sprint Communications Co., L.P.*, 1996 WL 33405972 at *2 (E.D. Pa. Sept. 17, 1996) (in the Third Circuit the “key considerations” are: (1) the degree of fault of the party who destroyed the evidence, (2) the degree of prejudice suffered by the opposing party; and (3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party and, where the offending party is seriously at fault, will serve to deter such conduct by others in the future).

First, a company's policy must ensure that written notification be given to all affected owners, officers, directors, and employees of: (1) the possibility of a future litigation, (2) the filing of an actual litigation, (3) the receipt of a preservation letter from opposing counsel concerning potential or actual litigation, and (4) any court orders concerning document preservation. Such written notification should disclose the names of the parties, the nature of the allegations, the key employees who may maintain relevant records, and the employees and third parties who may be potential witnesses. The notification should attempt to define broadly what information and documents might be potentially relevant to the litigation, and the categories of paper and electronic records that must be preserved that may contain relevant evidence.

The notification must instruct employees that they are prohibited from altering, erasing, or hiding potentially relevant electronic records, and should direct the appropriate personnel (*e.g.*, the IT department) to cease routine recycling of backup tapes that may contain relevant records, if necessary and appropriate. The notification should also advise employees of the possible sanctions attendant to failure to properly preserve evidence. The notification also should provide the names and telephone numbers of the appropriate contact persons in management, the legal department, and outside law firms. The company must then take active steps to ensure that its employees understand and adhere to their document preservation obligations, pending the company's efforts to corral, review, and produce, the relevant files and records.

A company's burdens with respect to e-mail preservation will be eased substantially by existing routine procedures, described in Section I above, which ensure that all e-mails are captured, routed, and stored on easily accessible and searchable media such as WORM disks,

optical devices, and tapes. With such procedures in place, individual employees will be unable to delete from their hard drives what possibly may be the company's only copy of a relevant e-mail, thereby obviating the need or opportunity for hard drive inspection of the company's computers by opposing counsel's computer expert. Further, disaster recovery backup tapes need not be restored and searched at considerable cost, and those tapes may be recycled and overwritten in the normal course of business without fear that possibly relevant e-mails are being erased, thereby saving further substantial costs.²⁸

With the proper procedures in place, a company can substantially decrease its litigation-related costs and anxieties. Potentially relevant evidence can be quickly accessed and searched for relevance, and be subject to privilege review. Corporations and their attorneys then can be freed to focus on the merits of the litigation, and on substantive litigation strategy, unburdened by the mind-numbing and cost-intensive aspects of electronic discovery.

D. Additional Considerations

Finally, many companies, large and small, have implemented e-mail policies that require all e-mails, across all business units, to be deleted after a very short time period, *e.g.*, thirty days. The stated rationale for this approach is as follows: if all e-mails are routinely and systematically deleted pursuant to a written company policy, then e-mails will not exist to be discovered in litigation. Such a policy purportedly serves the goals of eradicating potential "smoking-gun" evidence, and reducing, if not eliminating, the potential costs of electronic discovery.

²⁸ In *Wiginton*, defendant calculated that it would cost the company \$12,500 a day for new tapes to replace existing backup tapes that were the subject of discovery and could not be overwritten. See 2003 WL 22439865 at *3 and note 3.

This approach is defective because it does not ensure that all copies of internal or external e-mail are actually destroyed. With respect to internal e-mails, employees may download e-mails onto floppy disks, forward them to off-site locations, or print and retain hard copies. With respect to external e-mails, at least one copy will exist on a hard drive or backup tape of a third party over whom the company exercises no control. And, as discussed earlier, e-mails are not instantly “deleted” and cleansed from the company’s computer system upon the push of a delete button, but instead they linger on the computer’s hard drive as “residual data” until overwritten.

Further, this approach is disastrous for regulated companies that are required to maintain e-mails for a specific period.²⁹ A thirty-day purging policy also raises serious concerns for public companies under the Sarbanes-Oxley Act of 2002 and the SEC rules issued thereunder, because the policy could have an impact on the company’s “internal controls,”³⁰ and could expose the company to potential criminal charges for obstruction of justice.³¹

²⁹ See, e.g., SEC Release No. 34-46937 (Dec. 3, 2002) (Deutsche Bank, Goldman, Sachs, Morgan Stanley, Salomon Smith Barney, and U.S. Bancorp each fined \$1.65 million for failing to maintain all business-related e-mails for three years as required by SEC Rule 17a-4, insofar as these firms systematically discarded, recycled, and overwrote back-up tapes and other storage media containing the e-mails, and/or systematically erased all e-mails on the hard drives of personal computers of departed employees).

³⁰ Certain companies may not be able to properly maintain internal control over their financial reporting if they fail to review, and otherwise promptly delete, any and all e-mails related to internal accounting. Systematic deletion of all e-mails related to internal accounting might constitute a “material weakness” in a company’s internal financial controls under Section 404 of Sarbanes-Oxley, thereby requiring disclosure of such weakness in the company’s public filings.

³¹ Under Sarbanes-Oxley Section 802, a court may impose a twenty-year prison sentence against a defendant who has destroyed any document (e.g., deleting an e-mail) “in contemplation” of a federal investigation or “matter” that may not yet exist, if that such person’s intent was to “impede, obstruct or influence” such future matter. Presuming the inevitability of a federal investigation into the financial activities of any large public company, companies and their officers who adopt policies requiring systematic deletion of all corporate e-mails, within weeks of their creation, for the very purpose of preventing possible adverse evidence from falling into the hands of federal investigators, may be subjecting themselves to possible criminal prosecution and lengthy prison terms.

And finally, and most importantly, the approach represents a head-in-the-sand approach to corporate governance. Simply put, non-management of e-mail is mismanagement of e-mail. And given the central role that e-mail evidence has played in numerous recent major scandals, non-management of e-mail may well be mismanagement of the company itself. The first time senior management learns of misconduct evidenced in a company e-mail should not be when that e-mail is attached as Exhibit A to a multi-million dollar complaint, or when it is reproduced and quoted at length in the Wall Street Journal.

C
O
R
P
O
R
A
T
E
A
R
T
I
C
L
E
S

IT'S A FRIGHTENING PROSPECT, but true. In today's era of enhanced scrutiny of corporate activity, many companies are operating in the dark when it comes to records management. Some don't have a handle on how many and what types of records they have, where they are maintained and by whom, and even whether they still exist.

This places companies in a dangerous predicament if federal regulators come-a-knockin' with a subpoena in hand or if a party in litigation files a discovery demand. Simply throwing up your hands and shrugging your shoulders when asked to produce documents won't earn you the leeway you seek—but it could well invite civil and/or criminal ramifications. Developing and enforcing a records retention policy is something that you should have done yesterday—or you risk finding yourself and your company on the front page of the newspaper tomorrow.

If you're feeling a little anxious because you're behind the eight ball on this task, don't worry. This article will lay out the steps you need to develop, maintain, and enforce a records management program, and will help you get your corporate house in order.

How To Do Records Management for Maximum Protection

RECORDS MANAGEMENT: WHOSE JOB IS IT ANYWAY?

No matter the size or significance of the case, it always seems to come back to the documents. I have found that juries seem to find the greatest credibility in the written word. It is that document that is flashed before the jury that can make or break the case. And, as we have seen so vividly with the Arthur Andersen matter, documents—and most importantly retention programs—can mean life or death for a company and a person's career.¹

Ron Levine—Herrick Feinstein, LLP

Quotes like this one always seem to strike a nerve in the ranks of in-house counsel, whose scope of responsibilities has dramatically expanded over the past few years. Among various other tasks, in-house counsel may be charged with developing, implementing, and enforcing a corporate records management policy.

But as corporate obligations to establish and strictly enforce corporate records policies are intensifying, many companies are establishing records management policies that simply cannot be enforced or lack the procedural requirements that enable enforcement. That's because many companies don't appreciate what a solid records management policy can and should accomplish.

On the surface, a records management policy should advise a company how to:

1. **Keep** records long enough to meet requirements.
2. **Locate** records when needed.
3. **Protect** records when needed.
4. **Destroy** records as soon as they have met the retention requirements.

These basic records management requirements are essential to protect corporate interests, reduce legal risks, and eliminate unnecessary costs. The sad truth is that many companies have enacted records management policies that don't come close to meeting these four objectives. As they nervously watch their peers get walloped with huge fines and settlements stemming from a failure to produce records owing to negligence or malfeasance, company officials fret that their own corporate policies are ineffective to shield them from similar publicity and/or liability.

And it appears that they may have reason to worry.

According to a recent survey, over 80 percent of

the survey respondents do not believe their corporation's records policies are adequate, and over 90 percent do not feel the policies are meaningfully complied with in the normal course of business. (See "2004 ACC Records Management Survey Highlights," p. 91). For such an important corporate initiative and obligation, these are dismal statistics.

When companies look at their existing records policies and programs, they are often overwhelmed by the long list of opportunities for improvement. If you find yourself in such a category, don't despair. Many companies are in your shoes. Knowing the three issues that pose the greatest challenge to a company's efforts to implement and enforce a records management policy will help you avoid those pitfalls and the resulting liabilities. These issues are: developing and maintaining an enforced corporate records program; establishing and implementing legal "hold" management; and establishing a protocol for handling electronic records.

Developing and Maintaining an Enforced Corporate Records Program

Executives from all levels agree that records management policies are probably the one part of corporate governance that is uniformly neglected. Seventy-six percent of corporate counsel indicated that their company has a records policy; however, only 18 percent said the policy is actually enforced. Companies must develop a solid records program, and be able to establish that the requirements and controls of the program are standardized across the entire organization. The program must be applied to all record types regardless of the media, and enforcement must be a consistent part of the normal course of business.

Failure to approach the need for enforcement from both a senior management and budgetary perspective places a company at the mercy of employees who may or may not comply with the records program. In most cases, records policies set at the corporate level leave it to hundreds or even thousands of individuals to interpret the policy and determine what constitutes compliance, which is likely to yield haphazard compliance at best.

Establishing and Implementing Legal 'Hold' Management

As courts' and regulators' tolerance of excuses for

untimely and incomplete record production diminishes, it is imperative that legal departments be able to quickly locate and protect requested records. Companies without proper “hold” capabilities risk serious criminal and civil exposure if records have been destroyed or cannot be located when subpoenaed by prosecutors or requested by a litigant in discovery. According to Whitney Adams, general counsel at Cricket Technologies, there is very little tolerance for noncompliance. “The courts have made it clear that routine document retention practices and good intentions won’t protect a company from sanctions should relevant electronic information be destroyed.”²

THE COURTS HAVE MADE IT CLEAR THAT ROUTINE DOCUMENT RETENTION PRACTICES AND GOOD INTENTIONS WON’T PROTECT A COMPANY FROM SANCTIONS SHOULD RELEVANT ELECTRONIC INFORMATION BE DESTROYED.

Despite the enormity of the risk, many companies out there are apparently operating without an adequate legal hold mechanism. According to the survey, 70 percent of the companies send records hold notices to their employees when records must be protected for litigation or examination, but only 8 percent actually require employees to respond to the notices and effectively manage the records protection process.

But in order to effect legal holds, companies must have a mechanism for doing so. However, few organizations can quickly identify the records needed to support legal and investigative demands, rapidly notify the people who control those records in order to preserve or produce the relevant records, and then manage legal holds for records across all media types and applications.

Establishing a Protocol for Handling Electronic Records

The existence of several types of electronic records with differing levels of risk and different

enforcement issues requires that companies adopt a multifaceted approach when establishing a protocol. For example, it is necessary to identify which systems were used to create the documents in order to know which protocol is the most appropriate. Electronic records created on large-scale systems like Oracle, SAP, and PeopleSoft are handled differently than user-controlled electronic records on desktop applications.

It is also important to define what types of records fall within a certain category. General terms don’t always suffice to identify the vast array of electronic records that can exist within a company. For instance, when most people refer to electronic records, they may be referring only to email communications, voice mail records, and email records. But depending on the system and management culture, a subset of email records control could also include instant messaging trails left with off-site companies. These different types of records may require separate handling protocols.

For example, establishing a protocol for email and voice mail is more difficult than for other types of records because employees have a great deal of discretion and many opportunities to circumvent records management policies. The problem is compounded by the fact that companies have generally been unwilling to take a tough stand on policy violations, except in the most extreme cases.

A records management policy is only as good as its terms, and it’s absolutely no good if it isn’t enforced. The following discussion will help you establish a policy, and enforce it as well.

KEEP, LOCATE, PROTECT, DESTROY

Records management programs must enable corporations to:

1. Keep records long enough to meet requirements consistently throughout the entire organization and across all media types. To do this, a company must know what record types it has and how long each must be kept. Counsel must also understand the company’s current IT systems, and should consult with IT personnel on how to implement a complete systemwide hold if necessary under regulatory or “duty to preserve” requirements. Companies must make reasonable efforts to keep records

2004 ACC RECORDS MANAGEMENT SURVEY HIGHLIGHTS

In May 2004, the Jordan Lawrence Group conducted a survey of ACC members to gather information related to common records and information management issues facing corporate legal departments. A full report of the results of the survey is available at www.jlgroup.com and www.acca.com. The following is a portion of the data gathered from 240 corporate counsel responses.

COUNSEL RESPONDED: **PERCENTAGE:** **COUNSEL RESPONDED:** **PERCENTAGE:**

CORPORATE RECORDS POLICY

Does not have a records management policy	24
Has a policy but no enforcement	41
Has a policy and keeps it enforced	18
Requires sign-off for verification of employee policy review	5
Conducts mandatory training for employees	5
Disciplines employees for noncompliance with their policy	6

GENERAL RECORDS MANAGEMENT PRACTICES

Has difficulty finding records when needed	48
Can easily find records when needed	20
Does not have records classified into logical standards	51
Has most of their records classified	14
Cannot identify who owns or controls records	42
Can easily identify who controls their records	3
Has a retention schedule that is insufficient or outdated	26
Has no records retention schedule in place	18
Keeps records longer than necessary company-wide	52
Allows employees to set record-type names	36
Employees are inconsistent in complying with the policies	47
Employees are in compliance with records policies	9

RECORDS DESTRUCTION

Destroys records "as needed"	63
Never destroys records	8
Allows employees to destroy records they control "as needed"	73
IT destroys records "as needed"	63
Storage vendors never destroy records	25
Employees determine retention and destruction	40

EMAIL MANAGEMENT

Auto-deletes email	28
Restricts email by size	36
Classifies email according to set records standards	3
Deletes email backup according to retention requirements	28
Has email policy in place	46

LEGAL RECORDS RESEARCH/PRODUCTION

Ranked their legal staff as the top source of support for research	38
Ranked their finance department as the top source of support for research	18
Ranked their records management department as their top source of support for research	8
Relies most often on paper records located in off-site facilities	59
Relies most often on paper records located on-site within departments	46
Relies most often on electronic records for research	22
Relies most often on email records for research	12
Sends legal hold orders to their employees	70
Requires employees to respond to legal hold orders	8

AUDIT

Never audits storage vendors	48
Departments "self-audit" their compliance	59
Performs audits on compliance through the Internal Audit department	51
Never audits compliance with records policies	39

RECORDS CONTROL RESPONSIBILITIES

Legal is responsible for development of their records program	65
IT is responsible for development of their records program	32
Records Management is responsible for development of their records program	24
Records Management has no responsibility for any part of their records program	20
The legal department's participation and responsibilities regarding their records program have increased following Sarbanes-Oxley	48

AREAS OF RISK AND CONCERN

Ranks litigation and discovery as the top risks related to records management	60
Ranks excessive costs and litigation as the top concerns regarding records management	56
Are very satisfied with their current records program	4
Are less than satisfied with their current records program	80

*From this point on . . .
Explore information related to this topic.*

ACC RESOURCES ON RECORDS MANAGEMENT:

- “Records Retention: Enforced Corporate Records Programs,” an ACC InfoPAKSM from which much of this article is drawn, available on ACCA OnlineSM at www.acca.com/protected/infopaks/records/INFOPAK.PDF.
- “Sample Records Retention Plan and Schedule,” available on ACCA Online at www.acca.com/protected/forms/records/retentionplan.pdf.
- “Creating a Blueprint for an Effective Records Retention Program,” an ACC webcast replay, available on ACCA Online at www.acca.com/networks/webcast/webcast.php?key=20040701_3763.
- ACC has developed a policy on e-discovery, available on ACCA Online at www.acca.com/public/accapolicy/ediscovery.pdf. ACC has also testified before the U.S. Courts Committee regarding needed changes to the guidelines on issues related to records retention practices—read the comments on ACCA Online at www.acca.com/public/comments/testimony.pdf.
- Check out ACC’s “Leading Practices in Information Management and Records Retention Programs: What Companies Are Doing,” available on ACCA Online at www.acca.com/protected/article/records/lead_infomgmt.pdf.

If you like the resources listed here, visit ACC’s Virtual LibrarySM on ACCA OnlineSM at www.acca.com/resources/vl.php. Our library is stocked with information provided by ACC members and others. If you have questions or need assistance in accessing this information, please contact Senior Attorney and Legal Resources Manager Karen Palmer at 202.293.4103, ext. 342, or palmer@acca.com. If you have resources, including redacted documents, that you are willing to share, email electronic documents to Director of Legal Resources Julianne Bramesco at bramesco@acca.com.

at least as long as various federal, state, and other requirements dictate.

Meeting this requirement, however, doesn’t mean that companies should keep records forever. The obligation is to retain records as long as they have to be kept—and no longer.

2. Locate records quickly and effectively when they are requested. Regulating authorities require that records be available for a specified term, and expect that companies will adhere to those retention schedules. Given the increased frequency with which corporations are finding themselves in prosecutors’ cross hairs, it is important to meet those expectations. Companies must be able to quickly and effectively find records regardless of the media or storage facility in which they exist. Regulators who believe that a corporation has ready access to its records can quickly conclude that failure to produce records on demand amounts to corporate malfeasance. The consequences of such an assumption can be devastating for a corporation and its officers.

3. Protect records when they are subject to litigation or examination. Companies must be able to enact accurate legal holds to protect records that are or may be subject to pending or imminent litigation, investigations, or examinations. To meet this requirement, companies must be able to immediately identify the relevant records, notify the records’ owners, and shield the affected records from the regular destruction process. The hold status of the affected records must be communicated to all responsible parties—both internal and external. Compliance with the order must be tracked and monitored, and the hold order must be lifted once the matter has been resolved.

4. Destroy records when they become obsolete. Companies must systematically and nonselectively destroy records once the appropriate retention requirements and protection needs have been satisfied. Most companies apply records destruction practices inconsistently. Sixty-three percent of the companies who responded to the survey report that they destroy records “as needed,” rather than based on consistent application of an approved retention schedule. Seventy-three percent of companies allow employees to destroy records “as needed.”

It’s a simple rule: records that have met their retention standard should be disposed of. Failure to do so puts a company in an unnecessarily danger-

ous situation and causes it to incur unnecessary storage costs. Even more compelling, however, is the possibility that obsolete records that have not been destroyed could be subjected to legal discovery actions. In the absence of a policy of systematic and nonselective destruction of obsolete records, regulators will presume that all records still exist, regardless of their age.

It is also important that records be disposed of in accordance with industry practices and regulations that preserve the security of their information.

How to Satisfy ‘Who, What, Where, and When’

A company cannot meet its legal records retention obligations without exercising the discipline to capture, standardize, and manage important information about its records. Gathering this information and keeping it updated is simple—but absolutely critical—for corporate health and protection.

A company must identify:

1. What types of records are kept. Companies must know what record types are retained across all media. But most don't. Fifty-one percent of companies surveyed do not have records classified into logical standards.

Most companies have between 500 and 1,500 unique record types. Knowing those record types provides the baseline for creating a comprehensive, practical, and appropriate retention schedule. It also builds the first two enforcement pillars—what records can be “called” from this point forward and “how long records are to be retained” as dictated on the retention schedule.

After this information is developed, the database must be kept current to reflect the changing dynamics of new record types, abandoned record types, and record types that combine or separate with technology changes. The names, descriptions, life cycle, operational need, and other information elements of these records can only be obtained from the people who use them in their day-to-day work.

2. Who controls each type of record.

Unfortunately, even when the legal department is able to determine which record types need to be protected, it is often difficult to immediately identify and notify relevant personnel of their obligation to protect those records. After the responsible persons are identified, however, it is essential that companies implement procedures to immediately notify

them of document requests, track their receipt of the hold order, and monitor their compliance.

3. Where records are retained. Only 3 percent of companies surveyed said they can easily identify who owns needed records. Those are abysmal statistics and virtually guarantee a company's inability to comply with legal requests for documents. While research shows that the vast majority of records—95 percent—will never be needed, it is impossible to know which 5 percent will be needed. This makes the information about the records more valuable than the actual records themselves.

BY SETTING STANDARDS AND AUTOMATING ENFORCEMENT, RECORD TYPES THAT ARE INVENTORY-TOLERANT CAN BE EASILY CONTROLLED. THIS DISCIPLINE YIELDS SIGNIFICANT COST CONTROL BENEFITS, REDUCED LEGAL RISKS, AND EXCELLENT ACCESSIBILITY.

Companies must be able to immediately locate records within the organization regardless of the media type or geographic location. If records are presumed to still exist but cannot be located, records production becomes either impossible or unnecessarily expensive. Neither situation is acceptable to prosecutors or opposing parties, much less corporate officers or shareholders.

4. When records become obsolete. Most companies over-retain rather than under-retain records. However, very few records require permanent retention. The vast majority of records quickly become eligible for routine and nonselective disposal, in accordance with the approved policy. Knowing what records still exist facilitates a timely and efficient document production effort.

Records at many companies will reside on hundreds of applications and may be housed in various facilities. It is essential, however, that information about the corporation's records be centralized on a common system that will serve as the corporation's overall “enforcement hub,” containing all the information about all the company's records, record types, applications and vendors used, and other standards. Once this knowledge becomes part of

the corporate records program and policies are actually enforced, an organization can expect to realize dramatic reductions in legal risk exposure and costs related to records retention, management, research, and production.

Inventory-Tolerant and Inventory-Resistant Records

A company's ability to meet the four corporate requirements will also be impacted by the nature of the document—is it inventory-tolerant, or inventory-resistant?

A. Inventory-Tolerant Record Types (*Records Under Corporate Control*)

Records are inventory-tolerant when they are or could be controlled from a centralized perspective.

These records are characterized by the following traits:

1. They have naming standards that are adhered to and cannot be violated. Inventory-tolerant record types are those that are retained in strict conformance with the naming standards that are approved and set forth on the retention schedule. Employees have no discretion with regard to how records are classified—the predetermined record-type names included in the retention schedule are the only options allowed.

2. Control and ownership of each record and record type are always known. Knowing who has control or ownership of any record type is as simple as a few keystrokes in the enforcement hub.

3. The location of any record is always certain. Inventory-tolerant records are held in controlled inventories using strict database management discipline. This discipline can be applied to some paper records and to some electronic records, but not all.

4. Retention and ultimate disposal is a strict function of the approved retention schedule, rather than a function of employee discretion. Inventory-tolerant records will strictly conform to established retention standards, as employees and other parties have no discretion to assign retention periods or make ultimate disposal decisions. Retention and disposal criteria are automated and systematically applied in the normal course of business.

There are two types of inventory-tolerant records: (1) “native” electronic records and (2) boxes of paper records held in storage warehouses.

Native electronic records. The names of these

records can be standardized, their control and whereabouts can always be certain, and retention can be strictly complied with once retention periods are appropriately established. Examples of such records include those within large-scale financial and human resource systems.

Paper records in warehouses. These records can be stabilized by ensuring that all records are stored under standardized names, and that user discretion is eliminated for ongoing naming and classification, setting retention periods, and approving routine destruction. As users of storage services and storage vendors will probably lack the self-discipline to ensure strict compliance with standards, this regime needs to be automated and centrally monitored in order to make enforcement reliable. If automation is not possible, some form of centralized records intake to ensure accessibility remains critical to meet potential records production requirements.

By setting standards and automating enforcement, record types that are inventory-tolerant can be easily controlled. This discipline yields significant cost control benefits, reduced legal risks, and excellent accessibility.

B. Inventory-Resistant Record Types (*Records Under Employee Control*)

Unfortunately, many record types are not tracked by inventories. From an enforcement and control perspective, they are inventory-resistant.

The characteristics that make records inventory-resistant are:

1. The records are detached from any relationship to a centrally tracked and standardized control process.

2. Employees usually control the records and determine what they are called, where they are filed, how long they are kept, how many copies exist, and when and if the records are ever destroyed.

3. The company has lost control of the records, including what records still exist, who they belong to, how old the records are, and what retention obligations still exist.

Voice mail and email are the most dangerous of all inventory-resistant record types. Both have specific characteristics that make them particularly problematic and consequently dangerous. For example, employees are able to send and receive email

SELF-ASSESSMENT OF ENFORCEMENT

These are some of the indicators to assist a company in detecting the level of enforcement of its records management program:

Identifying records

- Does the company have a complete accounting of every record type it generates or retains?
- Does the list cover record types on all media platforms (paper, digital, electronic, and so forth)?
- How did the company develop this list?
 - What validation is done?
 - How is it refreshed regularly?
 - How often?
 - Is verification and updating routine or unstructured?

Protecting records

- Is the identification of records subject to legal hold status—those tied to pending or imminent government investigation, litigation, or audit—easy or difficult?
- Does the company have the ability to quickly enact, enforce, and monitor legal holds on records, regardless of media platform?
- Has the company ever mistakenly disposed of records that should have been protected? Could it happen? Is it likely?
- Can the company, with reasonable confidence, identify specific record types needed, and identify who owns or controls them? Would contacting those people be simple, automated, and trackable—or difficult, requiring time and effort, and with no certainty of receipt or compliance?
- Has the company ever been fined, unnecessarily settled a case, or faced other consequences owing to poor production capabilities?

Retaining records

- How does the company audit compliance with the retention schedule?
- Has anyone been disciplined for violating the retention standards?

- How current is the retention schedule? Does it cover all record types, across all media platforms? Is it impossible to comply with or difficult to enforce? How often is it verified and updated?
- How strong a stand would the company take on compliance if it believed that legal production costs, legal fees, and settlements could be cut by millions of dollars a year?

Electronic records

- Does the company retain too many electronic records?
- What are the legal and cost implications?
- Does the retention schedule cover electronic records?
- How is routine destruction activated and audited?
- Has any employee ever violated the company's email policy? Was the violation about content, usage, under-retention, or over-retention?
- Does the company treat content and usage matters more urgently than compliance with retention requirements? If so, why?

Unnecessary costs

- What is the estimated cost of over-retention of records in unnecessary research costs, settlements, and adverse inferences?
- Does the company retain too many records in warehouses? What are the implications?
- Could old records come back to haunt you in litigation?
- What has been the cost of migrating obsolete records to new storage or applications?

Monitoring compliance

- How many audits have been done in the past five years to benchmark volumes?
- Has any vendor ever lost or mistakenly disposed of records?
- All records-related efforts should point toward assuring that these obligations are met, first and foremost.

and voice mail with little or no immediate oversight. Moreover, the instant that an email or voice mail is sent or received, it can be simultaneously copied, sent to a noncorporate address, sent to someone

else, printed to hardcopy, saved to alternative media, and moved to a subfolder or other storage location. Finally, senders and receivers of an email communication can unilaterally transform an unnecessary or

even inappropriate communication into a discoverable corporate record by simply saving the communication, filing it, sending it elsewhere, or allowing it to be backed up onto email servers.

Emails: A Troublesome Lot

Emails are particularly problematic. In the case of this medium, none of the important records management requirements is met. Naming categories are not standardized, which makes it unduly difficult to retrieve and review the records. Ownership and control are lost, so it is difficult to pinpoint who has needed records. And email communications (records) can be anywhere at any time. They could be on backup tapes, saved to diskettes or CDs, or on an employee's home computer. Copies can be in many places simultaneously. This means that retention is impossible to control, as is routine destruction—even with retention standards set.

Instant messaging—a subset of email—poses its own unique problems. Instant messaging environments are relatively large corporate campuses, and lack a commitment to hand-held PDAs for a significant portion of the corporate employee base. The lack of control is made more difficult in that storage of messages is off-site and out of control of corporate personnel.

A Change in Status

Companies also inadvertently allow some inventory-tolerant records to become inventory-resistant due to poor oversight and control. Off-site boxes of

records should be easily controlled (and therefore inventory-tolerant). However, a company can allow records to become destabilized by allowing employees to: (1) assign them to groups outside the approved standards; (2) set retention periods with discretion (outside the approved standards); (3) circumvent routine destruction efforts at their own discretion; or (4) disregard adequate control and audit trails of record access while within the off-site storage site.

Off-site records can also be dangerous. For example, one company recently paid a \$10 million fine to the SEC due to poor off-site inventory control. But control of these records can be regained with simple enforcement efforts that usually yield a 40 to 60 percent immediate reduction in the excess volumes that most companies hold. Backup and archival tapes should also be inventory-tolerant, but may become inventory-resistant when indexing is out of control, volumes become difficult to ascertain, or resistance to changing the backup procedures is strong. Correcting past problems with tape management is also possible and is critical, as seen by the proliferation of legal settlements forced by adversaries demanding expensive reconstruction of old tapes.

OBSTACLES TO ENFORCING POLICIES

Although establishing and enforcing a corporate records policy are relatively simple matters, there are obstacles. Knowing what they are and how to overcome them is essential to an effective records management program.

Four Questions About Documenting Your Policy

Companies need policies that are clear and enforceable. Supporting procedures and systems must be in place for all media; retention schedules must be relevant, regularly updated, and—above all—spelled out in simple language.

While most companies have records policies in place, and many even have a written records retention schedule, few actually enforce records controls. Consequently, these companies have set a certain level of expected compliance that, in all likelihood, they cannot achieve.

To determine the adequacy of your company's records management documentation, ask these questions:

Come and establish your protocol for handling electronic records. Register for ACC's 2005 Annual Meeting on October 17-19 in Washington, DC. Topics include:

- Pitfalls & Landmines in Privacy and the Collection, Use, and Security of Personal Information;
- Workplace Privacy; and
- How to Manage Smoking Guns: The Ethical, Legal and Practical Guidelines for Document Retention.

For more information go to www.acca.com/am/05.

1. Does the policy clearly state that the company intends to retain records in compliance with federal, state, and other requirements?
2. Does the policy clearly spell out employee responsibilities and the consequences to the employee and the company for the employee's failure to meet these responsibilities?
3. Does the policy clearly inform employees that there are consequences for over-retaining records as well as for disposing of records too soon?
4. Is the retention schedule appropriate?

Specifically:

- Is it too long or too complicated to be of use?
- Is it more than one or two pages per department?
- Are record-type names less than 100 characters each or have descriptions crept into this column of the schedule?
- Are retention periods stated in simple monthly increments?

THUS, IT IS OFTEN IMPOSSIBLE TO ENFORCE A STANDARDIZED RECORDS MANAGEMENT PROGRAM WITHOUT A UNIFYING ENFORCEMENT SYSTEM IN PLACE BECAUSE THE RECORDS PLATFORMS ARE SIMPLY TOO SEPARATED, TOO INDEPENDENT, AND TOO INCOMPATIBLE TO WORK TOGETHER.

- Are retention periods numeric only, or have codes crept into the time periods?
- Are there over 2,000 record types listed on the retention schedule?
- Is the schedule for the entire corporation more than 100 pages long or does it weigh more than five pounds or occupy several binders?
- Do supporting procedures detail steps for the nearly two dozen day-to-day enforcement activities for enforcing a solid corporate records policy?

Having a records retention policy is only half the battle, though. Records policies are first and foremost about enforcement. It is essential, therefore, that a company's policy emphasize the perils of noncompliance. That means calling the employees on the carpet when they disregard the records man-

agement policy. This can be a major obstacle for some companies.

Tolerating Employee Misbehavior

Although it is unreasonable to expect employees to handle records appropriately if there is a poorly developed or nonexistent policy in place, even companies that have excellent documentation in place experience the problem of employees applying discretion at alarming levels. Why?

Employees ultimately care very little about records management issues. Companies don't bother to set rules, and when they do, they are unwilling or unable to enforce them. Forty percent of companies surveyed said their company's employees are allowed to set their own record-type names and retention. Seventy-three percent said they allow their employees to destroy records "as needed." However, only 6 percent have disciplined their employees for noncompliance.

When employees control compliance within the program, one thing is for sure—the result will be conduct that will be difficult or impossible to defend. It should be a goal for companies to remove employee discretion in records management. You can determine how much discretion employees have within a company regarding records management by asking these questions for all media (electronic records, email, paper, and backup tapes):

1. Does the company retain records for too long?
2. Are records maintenance costs rising in line with the growth of the company or at a higher rate?
3. Are records categorized in a manner that facilitates easy access and in accordance with the approved retention schedule?
4. Do employees have discretion to settle record naming categories, or are they confined to the approved record naming standards when they create or store records?
5. Do employees assign retention periods for records under their control, or are such periods assigned automatically and conformed to the approved company standards?
6. Do employees decide when records should be disposed of, or does destruction occur systematically in conformance with the company's retention standards?
7. How often is the records program audited, and are changes to the program made based on the results of the audit?

10 EMAIL BEST PRACTICES

Many companies have begun to adopt similar strategies and patterns for dealing with email, a major legal problem for corporations. The following steps have evolved as best practices:

- 1. Decide the general retention periods** for all nonessential (nonbusiness or legally required) email (30-day, 60-day, 90-day, and 180-day periods are all common).
- 2. Implement an auto-deletion system to eliminate nonessential email.** Because email has become a major tool in discovery that is successfully used by adversaries, it is critical that email volumes are kept at the minimum appropriate levels. Since electronic evidence firms bill by the megabyte or record, there's added incentive to keep email levels as low as possible. Do not use an outside archiving company for email—most companies will exponentially over-retain email if they lose day-to-day touch with how the volumes are growing.
- 3. Establish a subfolder classification scheme,** by department, that is representative of the retention schedule. Apply corresponding retention periods to subfolders. Departmental public folders should be established outside the email system for retaining business essential or legally required email only.
- 4. Implement a software solution,** if possible, that allows email retained in the subfolders to be culled and searched by content. This can cut down time and expense related to production.
- 5. Establish an automated notification process** that proactively pushes out the requirements of the policy to email users and requires a response. This further communicates to employees the critical nature of policy compliance and may help shield the company from the actions of rogue employees.
- 6. Establish firm consequences for noncompliance.** Poorly handled email is dangerous to corporations, and employees must be trained by policy, teaching, and ultimately by example. Decide the consequences the company can enforce for:
 - Keeping email too long;
 - Disposing of email too soon;
 - Misfiling (improperly categorizing) email;
 - Failing to comply with a legal hold notice;
 - Transmitting improper content; and
 - Storing email improperly or without authorization.
- 7. Document a strong email policy** that covers all of the above and ensures all supporting processes—backups and storage—are consistent with the policy.
- 8. Conduct corporate-wide training,** and update the program annually.
- 9. Monitor ongoing compliance** through regularly scheduled departmental audits.
- 10. Adjust the program as needed.**

Vendors Must Comply

Not only must companies meet the four legal requirements for corporate records maintenance, but any records-related services, equipment, and software used must support those legal obligations as well—even if they are performed by a vendor. It is the company's responsibility to ensure that this happens, not the vendor's.

A company's level of external obstacles can be evaluated by asking the following questions:

1. Do vendors have an incentive to recommend that the company dispose of records too soon? For

example, a secure destruction vendor could have such an incentive if they do not have a focus on policy enforcement.

2. Do vendors have an incentive to recommend or encourage over-retention of records? Data storage, records storage, document imaging, and media vendors all could benefit greatly from over-retention of records and data.

3. Do vendors have an incentive for research to be difficult or cumbersome? Storage vendors that allow user discretion in record naming or volume overruns could qualify under this category.

4. Are vendor operations periodically audited, and are changes made based on any negative findings?

Once you know the answers to these questions, you can then assess whether the corporation has a cohesive records management policy.

All Together Now

Corporations have hundreds of independent records platforms scattered throughout the organization, from email to content management and imaging systems, to paper records stored in off-site warehouses. All of these storage facilities and systems are actually silos of information where records are stored in such a way as to facilitate retrieval and research at some later date.

These records platforms operate independently of one another, retaining company records in different formats under different rules. Thus, it is often impossible to enforce a standardized records management program without a unifying enforcement system in place because the records platforms are simply too separated, too independent, and too incompatible to work together.

Although there might be legitimate and valuable reasons for maintaining these separate systems, they are bound to sabotage your efforts to keep track of all company records. Companies should develop and adopt standardized rules for record types across all platforms.

AS EASY AS 1, 2, 3

There are three steps to establishing an enforced records management policy.

1. Develop a program

Policies must clearly communicate these important items: (1) The corporate intention to comply with legal requirements; (2) the responsibility of employees to abide by such policies; and (3) the legal consequences to the employee and the company for noncompliance. A supporting framework (applied standards, procedures, and, where possible, enforcement automation) must be put in place. With a well-developed framework, it will be easier for a company to keep track of what record types are retained, who controls them, where they are located, and when they become obsolete. Here's how:

- In an automated system, new record types are captured and incorporated automatically into the program. Record types on all media can be included and tracked on a common system. Changes in retention requirements are simple to monitor and can be easily applied to all records.⁵ Obsolete record types are identified and automatically removed from the retention schedules.
- Record-type knowledge is automatically extended to cover new issues such as the use of alternative media, redundant retention of records, life cycles, business usage, and needs. Record-type knowledge is also automatically tagged to special needs situations such as the Sarbanes-Oxley 404 internal control requirements, the USA PATRIOT Act's rapid production requirements, the secure destruction requirements of Gramm-Leach-Bliley, and other industry-specific requirements.
- Ongoing compliance notices are automatically distributed to employees, requiring responses and compliance verification from all recipients and covering any area of concern or proactive enforcement such as: (1) annual policy update notices; (2) permanent retention reminders; (3) routine destruction orders; and (4) record-type update notices.
- Employee compliance expectations can be standardized so that employees do not have to remember what to do—they are proactively prompted to comply and then monitored to ensure that they actually do comply with the program directives. Legal holds can be automatically enacted from a single point, regardless of the record type, media, owner, location, or even vendors used. Records, however scattered around the nation or around the world, can be monitored, tracked, and disposed of consistently through a common, media-independent system.
- Employee discretion is completely eliminated for all variables that affect policy compliance.

The supporting framework ensures that stable records remain stable and that they are retained and disposed of properly. It ensures that the company proactively treats all records—including inventory-resistant record types—routinely with regard to proper retention, accessibility, and ultimate disposal. It also ensures the company's ability to enact accurate legal holds against any and all records that the company retains—on any media, anywhere in the world.

EIGHT QUESTIONS FOR ASSESSING RECORDS COMPLIANCE

In order to protect your corporate interests (assets, financial position, executives, employees, and so forth) and reduce legal risks and unnecessary costs, your company must be able to demonstrate consistent compliance with the following four requirements:

Keep records long enough to meet requirements consistently throughout the entire organization and across all media types:

Q: Are records retention requirements linked and applied to all records on all media?

Locate records quickly and effectively when they are requested:

Q: Can you accurately, quickly, and confidently find records when requested under litigation or examination?

Protect records when they are subject to litigation or examination:

Q: Can you effectively safeguard against records destruction or tampering when records are known to be (or suspected to be) part of a current or imminent litigation or examination?

Destroy records when they become obsolete:

Q: Can you demonstrate that records are destroyed consistently and systematically in accordance with your policies regardless of media type?

The only possible way to meet these four requirements is to capture, standardize, and continually manage the following four types of information about your company's records:

What record types your company retains:

Q: Do you know on a continual basis what record types are being retained throughout the organization?

Who controls each type of record:

Q: Can you quickly and easily determine whom to contact within your company to communicate instructions such as retention requirements, destruction, or legal hold notices?

Where records are located:

Q: Do you know what records are retained in various facilities and storage systems and where they are located?

When records become obsolete:

Q: Are your records retention requirements strictly and consistently applied to all records?

If you answered "No" to any of these questions, your company could potentially be exposed to unnecessary legal risks. You have the opportunity and responsibility, through a few easy steps, to increase your corporate protection and discipline by actually enforcing your records policy.

Where automation is not possible, counsel must still attempt to put these controls in place in order to enable a company to comply with the legal demands of a document production.

2. Implement the program

Once the initial policy elements are in place, the program must be launched. This includes employee training and the implementation of routine, documented practices supporting the corporate records policy.

Annual update training is proactive, and provides an excellent opportunity for the company to shield itself from the actions of rogue employees.

This system can be automatically scheduled, delivered, and tracked through the centralized enforcement hub.

Initially, companies will identify many records as eligible for immediate destruction—between 40 and 60 percent—based on updated record-type naming and retention standards. However, companies must ensure that any such records are not subject to pending or imminent actions that would supersede routine destruction. Such records should be shielded from loss or destruction through a specific, verified, and tracked hold notice.

Records eligible for destruction and not subject to a legal hold, however, should be disposed of

immediately (within 30 to 90 days), so that the integrity of the policy directives and retention standards is intact from the beginning.

Companies must also document the initial cleanup efforts, so that no appearance of selectivity or bias exists. The documentation should include:

- The reason the company has undertaken the updating or development of the new corporate records policy.
- How the policy and all components were developed, and the identities of those who participated in all aspects of program development.
- The time period during which the program was developed, the standards used for determining which records were eligible for initial disposal, and how the program was launched.
- The hold orders enacted to protect related records from loss or destruction, the timing of the initial destruction efforts, and the listing of all eligible records.

3. Enforce the program constantly

An enforced corporate records program is not a one-time effort. There are several tasks that must consistently be carried out if the program is to have an impact.

- Be proactive—use an automated system. If an automated system is not possible, counsel should contemplate a disaster plan and implement all of the possible elements of a policy to deal with that disaster on a nonautomated basis. Track all routine policy elements through the system. Deliver, track, and audit enforcement notices through the system.
- Demand compliance. Require all outside vendors to conform to the enforcement standards of the system. Do not allow deviation from the standards to reenter the program. Mandate annual employee training.
- Constantly refine the overall program. Annually update record-type knowledge. Monitor media migration to ensure that the record types used

at the company are always traceable by record-type name, media, ownership, and whereabouts. Annually revamp the retention standards at the record-type level by verifying the regulatory requirements and by comparing operational needs to the actual records usage level.

- Keep an eye out for trouble or for conduct by others that will get you in trouble. Discontinue work with vendors who obstruct the corporate policy and retention standards. Conduct periodic departmental audits to verify compliance with the policy. Consider reinforcing the seriousness of the policy by example and disciplinary action for policy violators.

ALTHOUGH THERE ARE MANY TOOLS AVAILABLE TO HELP COMPANIES CONTROL EMAIL AND ENHANCE THEIR ABILITY TO ENFORCE THEIR POLICIES, EMPLOYEES WILL CONTINUE TO HAVE THE ABILITY TO OPERATE OUTSIDE THESE CONTROLS.

- Don't follow the lead of the pack and let things slide. Only 6 percent of companies surveyed have actually disciplined employees for violations of their records policy. Are 94 percent condoning practices that could undermine the future of the company?

EMAIL: THE PROBLEM CHILD

According to a recent study by the American Management Association (AMA) and The ePolicy Institute, business usage of email is growing at 40 percent or more per year.⁴ The study also revealed that while 90 percent of employees send and receive potentially damaging email at work, 73 percent of their employers offer no email retention or deletion training. If this is true, almost three-quarters of the surveyed companies are relying on their employees to behave against their own instincts on when to keep email and when to delete it (especially when it's damaging).

Everyone is trying to find a fix for email control issues. The simple truth, however, is that you can't

control email in the same manner as other electronic records. Email systems that were originally designed as employee communications tools have been transformed into personal filing systems. Although there are many tools available to help companies control email and enhance their ability to enforce their policies, employees will continue to have the ability to operate outside these controls. Companies must therefore adopt means to effectively deal with these situations.

Some guidelines for developing company policy are listed below:

- The policy should direct employees on proper and improper use of the email system and content creation. It should instruct employees on the use or prohibition of use of instant messaging. The policy should also define email that falls under retention standards and non-essential email that must be purged immediately, such as general correspondence.
- For email that falls under the corporate retention standards, employees must be clearly informed that the company demands compliance with the retention and destruction requirements and must be told how the company intends to audit compliance.
- Since such a large portion of email is not needed, there are some simple solutions that the IT department can put in place, such as an auto-delete function. Obviously, however, the company will need to develop a way to protect the remaining percentage that truly does need to be retained.
- The policy should also lay out the potential consequences for violations of the policy, including retaining records for longer or shorter periods of time than the corporate standards or circumventing the policy by saving or sending email in an unauthorized manner.
- Don't go for the quick fix. In the past, many companies have tried to control email retention by restricting email directory space or size. This is similar to looking inside the company records warehouse and determining storage is at or near capacity. To avoid purchasing additional space, the company pulls and destroys boxes of records without regard to the legal requirements and consequences. Space-based decisions are almost always bad decisions, leading to inconsistencies that compound records control problems. Because email records will probably always be

under the control of employees—at least for the foreseeable future—they will always be inventory-resistant records. As such, the best approach for most companies is to create a consistent policy with clear instructions to the employees. This shifts the accountability and responsibility to the employees and builds a more defensible position for the company.


USE TECHNOLOGY TO SUPPORT ENFORCEMENT

In an ideal world, all records and every piece of information created at a company would be inventory-tolerant. The notes used in creating a contract, the minutes from yesterday's meeting, the various drafts of documents—all would be captured electronically and cataloged with the correct classification, storage location, and retention requirement. If these records were ever needed by Legal for a possible lawsuit, they could be located within seconds. The needed records would be protected from destruction until the matter was settled. Once the records became obsolete, they would be destroyed immediately.

In reality, however, companies are a long way from a completely inventory-tolerant records world. In fact, it will probably never happen. Most records that are high in volume or importance are under the solid control of the organization. Inventory-resistant records, however, will always exist throughout the organization, and there is nothing the company can do to control those records other than to give employees consistent and frequent instruction, and to monitor the results. Changing employee behavior requires time, consistency, and consequences for noncompliance.

Technology will always move closer to the ideal records management system; how much closer

depends on how much anyone is willing to invest. Theoretically, every office, cubicle, and conference room could be equipped with a scanning device to capture records as they were created. Every computer could capture, file, and classify every piece of input. This is obviously outside most companies' budgets.

But there is plenty of affordable technology available today that can help. Meanwhile, however, companies must continue to control what they can centrally and to shift accountability to individuals for managing the records they control. By identifying what records are kept, who controls them, where they are located, and when they become obsolete, a company will be able to develop a records management program that enables it to know how long to keep records, how to locate them when they are needed, how to protect them when they are or will be needed, and how to destroy them when they become obsolete. Don't delay developing and enforcing your records management program—and your corporate chronicles will have a happy ending. 

NOTES

1. From September 2003 ACC webcast, "Enforced Records Management is a Legal Requirement."
2. Whitney Adams and Jeffrey Jacobs, "Ghost in the Machine: Legal Developments and Practical Advice in an Age of Electronic Discovery," *ACC Docket* 22, no. 7 (July/August 2004): 48-72, available at www.acca.com/protected/pubs/docket/ja04/ghost.pdf.
3. Retention schedules are developed based on specific record types and are adapted to meet the most extensive retention schedule provided for by valid federal, state, business, or other requirement. User input is critical, since over 40 percent of record types have no regulatory retention requirements.
4. ePolicy Institute, "2004 Workplace Email and Instant The Messaging Survey," www.epolicyinstitute.com.

ACC Alliance Partners

The following Alliance partners offer services related to e-discovery. Be sure to mention that you are an ACC Member when inquiring about their services to receive your Alliance discount:

Cricket Technologies' electronic discovery services help companies manage electronic data for litigation.
www.CricketTechnologies.com

Jordan Lawrence Group works with companies to implement records retention programs.
www.JLGroup.com