

Electronic Discovery¹ **Employment Roundtable**

By Jim Barrett

Associate, Labor & Employment Group

October 19, 2006

I. WHAT IS ELECTRONIC DISCOVERY?

“Discovery” is the process by which two sides in a lawsuit exchange information about each other’s claims and defenses. Statistics show that more time is spent on discovery than on any other legal task and can represent anywhere from 50% to 90% of total litigation costs.²

“Electronic discovery” refers to litigants’ requests for documents that are stored in electronic form. It does not refer simply to email. Electronic discovery requests routinely require production of files residing on laptops, office PCs, network servers, floppy disks, personal digital assistants, CD-ROMs, MP3 players, Blackberries, cell phones, backup tapes, flash memory cards and devices, and other archive media.

Electronic discovery also refers to metadata or digital “fingerprints” that, with the assistance of computer forensics, can be used to determine background information regarding when electronically-stored documents were created, modified, sent, viewed, etc. This information can often be more important than the substance of the document itself.

Example: *Williams v. Sprint/United Management Co.*³ In a class action lawsuit, employees alleged age discrimination in layoffs. Defendant produced Excel spreadsheets showing reduction-in-force calculations in a static image format that eliminated the mathematical formulae behind the spreadsheets, text that exceeded cell size, and metadata. The court held that the defendant had an obligation to preserve and produce the Excel spreadsheets in their native format or take other measures to preserve and produce non-apparent information, as it was reasonable assume that the calculations, text, and metadata would be relevant.

Example: *Lee v. Oracle Corp.*⁴ An Oracle employee, Adelyn Lee, successfully sued Oracle for wrongful termination, claiming that she was fired by her supervisor after she refused to have sex

¹ This memorandum contains a summary of information obtained from laws, regulations, court cases, administrative rulings, and legal publications, and should not be viewed or relied upon as legal advice. Ater Wynne LLP urges readers of this memorandum to consult legal counsel regarding specific legal issues and factual circumstances.

² 1 Employment Discrimination Law and Litigation, sec. 14.27.

³ 230 FRD 640 (D. Kan. 2005).

⁴ 1999 WL 595455 (Cal. App. 1999).

with Oracle CEO Larry Ellison. During the discovery process, Oracle's lawyers found an email in which Lee's supervisor told Ellison "I have terminated Adelyn per your request." Oracle settled immediately for \$100,000. However, Lee's supervisor insisted that he never sent the email. By using forensic analysis to determine when and how the email was created, Oracle later was able to show that Lee had broken into Oracle's computer system, accessed her supervisor's email using his password, and forged the email. Oracle successfully sued Lee for perjury and falsification of evidence.

II. WHY IS UNDERSTANDING ELECTRONIC DISCOVERY IMPORTANT?

A. Prominence in Litigation.

More than 80% of corporate communications are sent via email and, according to one statistical study, more than 99% of new information currently being created and stored is done so electronically.⁵ Each person produces almost 800 megabytes of recorded information each year, 92% of which is stored magnetically on computers or other storage media (imagine a stack of books 30 feet tall).⁶

Electronic discovery has quickly become a critical focus of litigation. According to a 2006 survey by the American Management Association, "24% of organizations have had employee email subpoenaed, and 15% of companies have gone to court to battle lawsuits triggered by employee email."⁷

Example: *Vandell v. Chevron*.⁸ Chevron paid female employees \$2.2 million to settle a sexual harassment lawsuit stemming from an email circulated by male employees. One of the offending emails contained a "joke" sheet listing "25 Reasons Why Beer Is Better Than Women."

Example: *Harley v. McCoach*.⁹ Plaintiff was able to substantiate her claims of inappropriate sexual conduct by co-workers when she produced an email message identifying her as "Brown Sugar."

B. Take Steps to Limit Your Liability.

New Federal Rules: The prominence of electronic discovery has led to a change in the Federal Rules of Civil Procedure that will take effect on December 1, 2006. The two aspects of the new rule critical to every business are:

1. **The importance of having a document retention policy.** The new rules provide that "absent exceptional circumstances, a court may not impose

⁵ 2006 Workplace E-mail, Instant Messaging & Blog Survey: Bosses Battle Risk by Firing E-mail, IM & Blog Violators, http://www.amanet.org/press/amanews/2006/blogs_2006.htm (American Management Association).

⁶ Kenneth J. Walters, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 Northwestern J. of Tech. & Intellectual Prop., 173 (Spring 2006).

⁷ See fn 5, *supra*.

⁸ Cal. Sup. Ct., Civ. Case No. 945302 (1995).

⁹ 928 F. Supp. 533 (E.D. Pa. 1996).

sanctions under these rules on a party for failing to provide electronically stored information lost as a result of routine, good-faith operation of an electronic information system.” FRCP 37(f).

2. **The risks and advantages of having a document retention system that stores electronic information on media that is not reasonably accessible.** Under the new rules, a party is excused from providing discovery of electronically stored information that it identifies as “not reasonably accessible because of undue burden or cost.” Rule 26(b)(2)(B).

C. **The Consequences of Failing to Address the Management of Electronically Stored Data Can Be Very Expensive.**

Statistics show that more time is spent on discovery than on any other legal task. It can represent up to 90% of litigation costs in which it is actively pursued.¹⁰ If not properly managed, the sheer volume of electronically stored information greatly increases the potential costs associated with identifying, restoring, and reviewing documents.

In addition, failure to have an established procedure for managing electronically stored information in anticipation of, or during, litigation increases the risk of inadvertent destruction, which can result in monetary sanctions and/or an adverse instruction from a court.

Example: *Tapemorr, LLC v. Killion Enterprises*.¹¹ Judge Nachtigal in Washington County, Oregon, admonished a defendant for failing to preserve evidence on a computer and imposed attorney fees as a sanction:

If this were a case of a filing cabinet and what’s in the filing cabinet is an essential part of the case, and, “Oh, our regular business practice is, at the end of the week we throw everything out of the filing cabinet and burn it up. We didn’t know that you wanted this,” and although it’s the whole core of the case, that wouldn’t fly in any court at any time. But somehow because it’s a computer and all’s we did was delete it or write it over, it’s different. It’s not different.

* * * * *

This was about what’s on the computer. * * * Is there something on there? I don’t know. Do they have all of the emails? I don’t know. Without canvassing every possible business in the world, it’s hard to know what other e-mails are out there. * * * I’m not satisfied that 50,000 is a dollar figure that can be presented, but certainly reasonable attorney fees for bringing this to your attention is reasonable.

Example: *Accordia of Oregon, Inc. v. Bliss*.¹² In a case involving suspicious deletions of electronically stored information from home computers, Judge Lipscomb in Marion County ruled

¹⁰ 1 Employment Discrimination Law and Litigation, sec. 14.27.

¹¹ Washington County Circuit Court, Civil Case No. 044404 (Aug. 24, 2005).

¹² Marion County Circuit Court, Civil Case No. 05C18113 (Apr. 20, 2006).

that “any fact finder would have more than sufficient evidence to support an inference that material and damaging evidence was willfully destroyed by Defendants shortly after they were served with this lawsuit” and that the plaintiff would be entitled to a jury instruction to that effect. Further, the judge ordered the Defendants to pay plaintiff’s attorneys fees and costs as sanctions for destruction of evidence.

III. PLANNING FOR ELECTRONIC DISCOVERY

A. EMAIL USE POLICIES

The first step in limiting liability and protecting against damaging electronic evidence is to establish and enforce email use policies. The policy also should extend to blogs that your company operates.

1. Common issues.

- (a) Understanding the risks. A policy should educate employees about the risks to the employee and the company associated with the improper use of electronic storage devices, such as email and the Internet.

Examples:

- (i) Email encourages informality. Email can be easily forwarded, modified, forged, or sent to unintended recipients.
- (ii) Liability for libel, defamation, harassment, copyright infringement.
- (iii) Breach of confidentiality; waiver of privileges.
- (iv) Liability for spreading computer viruses.

- (b) Personal use limitations. Strictly business or “reasonable” use?

Examples:

“The purpose of internal communication systems, including email and access to the Internet, is to conduct company business. Personal use of these systems are to be kept to a minimum. Personal use of communication systems (including the Internet) that interfere with the user’s productivity or work performance, or the productivity or work performance of others, is prohibited.”

“Company’s internal communication systems, including email, voicemail, and access to the Internet, are strictly for business purposes. Use of these

systems to send personal emails or surf the Internet for non-business related reasons is strictly prohibited.”

- (c) Privacy expectations. Make it clear that employees do not have an expectation of privacy. Example:

“All of the Company's communication systems, including electronic mail, voicemail, Internet access, and electronic storage systems, are Company property, and are not confidential. The Company reserves the right to access, monitor, and review these systems at any time, and to read and retrieve messages.”

- (d) Content limitations. Set guidelines for proper and improper content. Examples:

“Email should be used in a respectful and appropriate way. The Company expects everyone who uses the email system to exercise good judgment and common sense with regard to mail generated both internally and externally. The Company's policies prohibiting discrimination and harassment apply equally to the email system.”

“Email may not be used for any commercial purpose other than Company business. Employees are not permitted to use the Company's email system for “spamming” (distributing commercial, religious, or political messages indiscriminately) or for pyramid or chain letters or other junk mail.”

- (e) Access and download limitations. Prohibit or limit the type of information employees may access, download or forward. Examples:

“Employees are not permitted to read, intercept, copy, use, or disclose email communications directed to others without express authorization. Accessing another employee's electronic mailbox without the latter's express permission is strictly prohibited.”

“Employees may not forward any email that is marked “confidential,” “privileged,” or that contains proprietary or sensitive company information.

“The Company's access to the Internet is to be used solely for Company business purposes. Authorized business use does not include sites that contain sexually explicit materials, news groups dedicated to hate or violence, gambling, shopping, or job searches. This list is not exhaustive. The Company reserves the right to access and review records of employee use of the World Wide Web.”

“Employees are not permitted to download any software or from the Internet without authorization from the Information Systems Department.

“Employees are not permitted to access or download any pornographic, obscene, or indecent material from the Internet.”

- (f) Misaddressing emails. Many companies require emails sent from the company system to carry a disclaimer to avoid liability for misdirected emails. Example:

“This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the company. Finally, the recipient should check this email and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this email.”

- (g) Storage/archiving protocol. The company should explain its document retention system to its employees. Example:

“All emails will be automatically deleted after 60 days. If you need to retain an email, the message must be moved to the folder “for archiving.”

- (h) Discipline/enforcement. The company should advise employees of the consequences of misuse of email and have them acknowledge the policy in writing. Example:

“Employees who fail to comply with this policy may be disciplined, which may include termination and/or legal action.”

2. Enforcing Electronic Communication Policies.

Once established, companies can and should actively enforce electronic communication policies to minimize liability. A recent survey revealed that three out of five employees admitted to surfing the Internet while on the clock.¹³ Of more than 500 companies that participated in another survey, 61% disciplined employees for inappropriate Internet use and one-quarter of them went so far as to terminate an employee.¹⁴

Email has the potential to be problematic, even when inadvertent mistakes are made. For example, Oregon’s Bureau of Labor and Industries (“BOLI”) recently addressed the inadvertent use of the word “butt” instead of “but” in an email addressed to an employee who was sensitive about her postpartum weight. BOLI’s advice:

Employer’s emails need to state things in as purely a factual manner as possible because communicating opinions, judgments or anything that could be interpreted

¹³ Melissa Pachikara, *Wipeout: The Dangers of Workplace Websurfing* (Sept. 28, 2006), at www.npr.org/templates/story/story.php?storyId=5697883.

¹⁴ *Id.*

as offensive or flippant in writing, without the benefit of the personal non-verbal interactions you can observe, are easily misunderstood.

Also, an investigation should be initiated to determine whether [the sender] is engaging in inappropriate workplace harassment by utilizing email as a vehicle for improper comments. Given [the sender's] use of the word 'butt' in his email, which you interpreted to be a reference to your backside, you should share the email with your supervisor so they might conduct the appropriate investigation to ensure that [the sender] is not engaging in harassing behavior.¹⁵

Courts will credit an employer's consistent enforcement of an email policy as an exercise of reasonable care. Examples:

*Schwenn v. Anheuser-Busch Inc.*¹⁶ Court dismissed sexual harassment claim when employer showed that it had promptly responded to an employee's complaint by issuing a warning to employees not to abuse email.

*Mieritz v. Hartford Fire Ins. Co.*¹⁷ Employee "witnessed" his Christian faith by including biblical quotes in emails to his co-workers, speaking directly to his co-workers about his faith, posting copies of prayers in his work area, and using a Christian screen-saver on his office computer. When the employee's position was eliminated along with three others, employee sued for discrimination on the basis of religion. The court granted the employer summary judgment when it was shown that the employee was aware of the company's policy prohibiting the use of company computers for "solicitation or proselytizing," but did so anyway. The court also found that nothing in the employee's religion required him to use the computer system to "witness" his faith, so there was no conflict between his *bona fide* religious beliefs and the company's computer policies.

*Daniels v. Worldcom Corp.*¹⁸ When an employee initiated a discrimination suit after receiving a racially offensive email, the employer avoided liability by demonstrating that it had taken prompt remedial action by issuing a disciplinary warning to the employee who sent the email and holding a company-wide meeting to discuss the policy on email use.

*Stuart v. General Motors.*¹⁹ An employee complained of sexual harassment in part because a computer in her work area contained pornographic program. GM responded by removing the computer, starting an investigation of every computer, interviewing 30 employees, offering to move the employee to another area in the same position, and updating the employee three times on the investigation. GM learned that the source of the program was a retired employee. It sent a letter and pamphlet to all employees describing its harassment policies. In dismissing the

¹⁵ http://www.oregon.gov/BOLI/TA/T_Newspaper_Columns.shtml (*he Trouble with E-Mail*, August 1, 2006).

¹⁶ 1998 WL 166845 (N.D.N.Y. 1998)

¹⁷ 2000 WL 422909 (N.D.Tex. 2000)

¹⁸ 1998 WL 91261 (N.D. Tex. Feb. 23, 1998).

¹⁹ 217 F.3d 621 (8th Cir. 2000).

employee's later suit against GM, the court cited favorably the prompt and thorough investigation and the republication of the harassment policy.

*Sherrod v. Commonwealth Edison Co.*²⁰ Court upheld company's decision to terminate a female employee who violated the company's policy prohibiting employees from downloading pornographic images and storing them on company's computers.

B. DOCUMENT RETENTION POLICIES

In discussing document retention plans, it is necessary to draw a distinction between "information," which broadly refers to all of an organization's tangible documents and data, and "records," which refers more narrowly to information that has some value to the organization requiring special attention concerning retention, accessibility, and retrieval. The determination of what information constitutes a business record typically is a function of law and company policy.

1. Retention of Records Required by Law.

Many federal and state laws affect employers' recordkeeping practices. Some of these laws apply to all employers, while others apply only to specified categories of employers or employees.

Types of Employment Records Required by Law

Type of Record	Law Requiring Retention
Job advertisements and internal job postings	ADEA, FLSA and ADA
Employment applications and/or Detailed Information on Applicants	ADA/Title VII ADEA, and OFCCP affirmative action regulations
Offers and hiring records	ADA, Executive Order 11246, Title VII, Vets Act
INS Form I-9	IRCA
Basic employee data (name, address, birth date, sex, etc.)	FLSA; many others
Promotions, demotions, and transfers	ADA, ADEA, and Title VII
Time cards	ADEA and FLSA
Payroll records	Oregon minimum wage law and unemployment insurance law, ADEA, Equal Pay Act, FMLA, FLSA, Internal Revenue Code
Records of leaves of absence and disputes regarding leave eligibility	FMLA
Reasonable accommodation records	ADA
Medical records	ADA, ADEA, FMLA, OR-OSHA and Civil Rights Act
Employee pay and benefit plans	FMLA, ERISA

²⁰ 2000 U.S. Dist. LEXIS 1626 (N.D. Tex. Feb. 4, 2000).

Type of Record**Law Requiring Retention**

Child labor information/certificates	ORS 653.310; 839-021-0170 et seq.
Employment contracts	Equal Pay Act and FLSA
Records and logs of occupational injuries, illnesses, and deaths	OSHA/OSEA
Employee exposure to toxic substances	OSHA/OSEA
Records of layoffs	ADA, ADEA, and Title VII
Employee terminations	ADA, ADEA, Executive Order 11246, and Title VII
EEO-1 and Vets-100 reports	ADA, Executive Order 11246, Title VII, Vets Act
Affirmative Action Plans and Documentation	Executive Order 11246, Vet's Act, etc.

2. Retention of Records Required by Policy.

Whether or not a specific law requires it, employers should keep certain employment records as a matter of policy because they are critical in many situations. For example, applicant records, including applications, resumes, test results, licenses, accreditation, references, background checks, drug test results, and any other documents considered in deciding whether to hire an applicant, should be retained.

BEST PRACTICES. The following are five principles developed by The Sedona Conference Working Group on Best Practices for Electronic Document Retention & Production (Sept. 2005):

Principle No. 1: A Retention Policy Must Be Reasonable Under the Circumstances.

There is no one-size-fits-all retention policy. Each organization must evaluate its needs, the laws that apply to its records, and the available technology to develop a reasonable record retention system.

Absent evidence that an organization has actual knowledge that specific information would be material to foreseeable claims or legal requirements, its best judgment generally will be respected. "It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under normal circumstances." *Arthur Andersen, LLP v. United States*.²¹

Having no record retention policy in effect during litigation will likely be viewed as unreasonable, contributing to the negligent destruction of relevant information. *See, e.g., Telectron, Inc. v. Overhead Door Corp.*²² ("The absence of a coherent document retention policy during the pendency of this lawsuit" was cited as leading to "possibly willful document destruction occurring in both routine and nonroutine manners . . .").

²¹ 125 S. Ct. 2129, 2135 (2005).

²² 116 F.R.D. 107, 123 (S.D. Fla. 1987).

Courts routinely examine “reasonableness” given the facts and circumstances surrounding the information or record at issue:

Example: *Lewy v. Remington Arms Co.*²³ Court noted that retaining appointment books for three years might be reasonable, while retaining customer complaints about product safety for three years might not be reasonable.

Example: *United States v. Taber Extrusions L.P.*²⁴ Government had destroyed documents related to government contracts under its document destruction policy. Court found that policy of destroying documents after 6 years and 3 months was reasonable on its face.

Compare: *Reingold v. Wet ‘N Wild Nev., Inc.*²⁵ Company’s policy of destroying documents before statute of limitations on potential – and foreseeable – claims expired was not reasonable.

Principle No. 2: Retention Policies should be realistic, practical, and tailored to the circumstances of the organization.

A. *No One Policy Will Fit Every Organization.*

Each organization’s retention policy will be different. Important contextual factors are:

- (a) The nature of the business;
- (b) The legal and regulatory environment of the business;
- (c) The culture of the organization;
- (d) Whether data within the organization is distributed or centralized;
- (e) Standard business practices and procedures within an industry.

Caution: As tempting as it may be, document retention policies should not be designed with the goal of hampering future litigation. Cases abound with cautionary tales of ill-conceived document retention policies that were viewed as vehicles for purging “bad” documents:

Example: *Broccoli v. Echostar Communications.*²⁶ An employer’s email retention policy mandated deletion of emails within 21 days and deleting all emails of terminated employees within 30 days. While the court did not view this policy as sanctionable, it was “extraordinary” and “risky.” The employer’s failure to suspend the policy after being placed on notice of potential litigation resulted in an adverse instruction to the jury that the employer had willfully destroyed relevant documents.

²³ 836 F.2d 1104, 1112 (8th Cir. 1988).

²⁴ 2001 U.S. Dist. LEXIS 24600 (E.D. Ark. 2001).

²⁵ 944 P.2d 800 (Nev. 1997).

²⁶ 229 FRD 506 (D. Md. 2005).

Example: *Rambus Inc. v. Infineon Techs. AG.*²⁷ Plaintiff plotted patent infringement litigation at the same time it implemented a document retention policy that included a “Shred Day” right before it filed its lawsuit. The court ordered discovery of the plaintiff’s lawyer’s files under the crime-fraud exception to the attorney-client privilege and the lawsuit was ultimately dismissed.

Example: *Kozlowski v. Sears, Roebuck & Co.*²⁸ The court held that a party cannot excuse itself from compliance with discovery rules by adopting a records management system designed to make discovery unduly difficult.

Example: *Reingold v. Wet ‘N Wild Nev., Inc.*²⁹ The court held that a one-season retention policy at a water park was unreasonable as “deliberately designed to prevent production of records in any subsequent litigation.” As a result, the court ordered a new trial and directed that an adverse inference instruction was appropriate.

B. Distinguish Between a Document Retention Policy and Disaster Recovery Policy.

The purpose of a business continuation or disaster recovery plans is different from the purpose of an information and records management program, and should not be used as a substitute for records and information management.

Many businesses routinely back up electronic information on tapes. Under the new Federal Rules regarding electronic discovery, information on such back-up tapes are presumptively considered “inaccessible” because of the difficulty and cost involved in restoring and searching them for relevant information. However, if a company relies on back-up tapes as part of its document retention policy, then it substantially increases the chance that a court will order that the company undertake the effort and cost of searching them.

Example: *Quinby v. WestLB AG.*³⁰ An employer ended up paying close to \$250,000 to restore and search backup tapes because it had moved key former employees’ emails to backup tapes after it should have anticipated litigation. Importantly, the employer was not guilty of “spoliation” or destruction of evidence. However, the court held that the employer had created its own expensive retrieval problem and should, therefore, bear the cost.

Principle No. 3: You do not need to save all electronic information ever generated or received.

There is no general requirement that businesses retain all information created or received. The U.S. Supreme Court has recognized an expectation that organizations will delete and destroy documents in the ordinary course of business. *See Arthur Andersen, supra*, 125 S. Ct. 2129

²⁷ 220 FRD 264 (E.D. Va. 2004).

²⁸ 73 FRD 73 (D. Mass. 1976).

²⁹ 944 P.2d 800 (Nev. 1997).

³⁰ 2006 WL 2597900 (S.D.N.Y. 2006).

(2005). Even during litigation, where preservation obligations are expanded, courts recognize that organizations are under no obligation to retain everything.

Example: *Concord Boat Corp. v. Brunswick Corp.*³¹ “To hold that a corporation is under a duty to preserve all email potentially relevant to any future litigation would be tantamount to holding that the corporation must preserve all email. . . . Such a proposition is not justified.”

An organization should determine the “lifecycle” of information and retain information only so long as it has value as defined by the organization’s needs or legal requirements. (As discussed later, this determine must be subject to suspension if litigation is reasonably anticipated.)

Retaining excess information can result in substantial costs to the organization. The more information that is stored, the more the organization may be directed to review and produce in litigation. It also can increase the cost of locating information. Example:

Company does not have an email retention and destruction policy and collects one million pages of email and attachments from 25 employees in preparing for litigation. All pages are converted and scanned at \$.20/page for \$200,000. Attorneys review the pages for relevance and privilege at \$.50/page for \$500,000. It is determined that 10% or 100,000 pages were relevant. If 50%-75% of the emails had no “retention value” to the Company, then the Company spent \$350,000-\$525,000 on processing documents that had no value and were retained for no purpose.

Courts will not draw adverse inferences from the destruction of documents that occurred pursuant to a reasonable policy. The new federal rules expressly incorporate a safe harbor for organizations who fail to produce electronically stored information “lost as a result of routine, good-faith operation of an electronic information system.” FRCP 37(f).

Example: *Willard v. Caterpillar, Inc.*³² The court held that the “good faith disposal pursuant to a *bona fide* consistent and reasonable document retention policy could justify a failure to produce documents in discovery.”

Example: *Vick v. Tex. Employment Comm’n.*³³ No adverse inference was drawn where documents were destroyed pursuant to Commission regulations governing disposal of inactive records.

Automatic destruction programs: Absent a legal requirement to retain information, organizations can implement retention and deletion periods for recorded communications. Some organizations proscribe space limitations (1 MB for email) or time restrictions (all non-folded emails will be deleted in 30 days). Organizations can set up instant messaging to prevent archiving of the typed conversation. However, it is critical that an organization have a means of managing emails and other information that qualify as “records” and that it be able to suspend the automatic destruction of documents whenever necessary.

³¹ 1997 WL 33352759 (E.D. Ark. 1997).

³² 48 Cal. Rptr. 2d 607 (Cal. Ct. App. 1995).

³³ 514 F.2d 734 (5th Cir. 1975).

Example: *Modaid Technologies Inc. v. Samsung Electronics Co., Ltd.*³⁴ The court sanctioned the defendant for failing to prevent its system from automatically purging potentially relevant emails after the lawsuit was filed. The court ordered that the jury be given an adverse inference instruction so that it could assume that the deleted electronic information would be harmful to defendant.

An organization also may implement a policy of recycling media that contain data retained for business continuation or disaster recovery purposes. Company's typically retain this information, such as backup tapes, much longer than is necessary to protect against a disaster.

Principle No. 4: An organization must develop and enforce procedures to address the creation, identification, retention, retrieval and ultimate disposition/destruction of information.

A. Implementing and Enforcing Policies Is Critical.

To be effective, document retention policies should be communicated in writing so that all employees understand their obligations and responsibilities. Roles should be defined within the organization to respond to unforeseen needs to retain information. The absence of a coordinated, defined policy can come back to haunt an organization in litigation.

Example: *Coleman Holdings Inc. v. Morgan Stanley & Co., Inc.*³⁵ The failure to coordinate the search for backup tapes led to late discovery of more than 2,500 tapes, and partial default judgment, which contributed to a jury verdict of \$1.5 billion in compensatory and punitive damages.

Example: *Zubulake v. UBS Warburg LLC*.³⁶ Failure to communicate within organization and with counsel led to late productions and loss of data, warranting adverse inference instruction; jury returned \$29 million verdict.

Example: *Landmark Legal Found. v. EPA*.³⁷ The EPA represented that it would preserve responsive materials, but plaintiff later established that the agency had failed to distribute a preservation order widely enough to include the IT staff responsible for preserving email backup tapes, individuals who had the requested data, or the acting administrator.

Example: *Thompson v. United States HUD*.³⁸ The defendant claimed that it "discovered" more than 80,000 emails on the eve of trial. The court prohibited the defendant from introducing information from these emails and defendant's counsel was prohibited from using them to refresh a witness's recollection or to prepare a witness for trial. Plaintiffs, however, were permitted the use of the emails and were invited to seek recovery of the costs of reviewing them.

³⁴ 2004 US Dist. LEXIS 23596 (D.N.J. July 7, 2004).

³⁵ 2005 WL 674885 (Fla. Cir. Ct. Mar. 23, 2005).

³⁶ 2004 WL 1620866 (S.D.N.Y. July 20, 2004).

³⁷ 272 F.Supp.2d 70 (D.D.C. 2003).

³⁸ 219 FRD 93 (D. Md. 2003).

B. Upper Management Should Be Actively Involved.

Courts may look to the level of support by senior management in determining whether a document retention policy is reasonable.

Example: *Danis v. USN Communications, Inc.*³⁹ In this case, the failure to take reasonable steps to preserve data at the outset of discovery resulted in a personal fine levied against the defendant's CEO.

Example: *In re Prudential Ins. Co. of Am. Sales Practice Litig.*⁴⁰ "The obligation to preserve documents that are potentially discoverable is an affirmative one that rests squarely on the shoulders of senior corporate officers."

C. Employee Education Is Essential.

Technology can reduce the number of human steps in determining what information is retained and for how long. An organization should consider the extent to which its retention policy should use electronic archives and automated tools. However, regardless of what policy is adopted, the organization must determine the most appropriate way of disseminating that policy to its employees and how best to train them. The policy should be revised and updated periodically.

Principle No. 5: A retention policy must mandate the suspension of ordinary destruction practices as necessary to respond to reasonably anticipated litigation.

An organization's document retention policy must recognize that, under certain circumstances, it must suspend its standard procedures to preserve potential evidence. Such circumstances include anticipated litigation, government investigation, or audit. Certain business events also may require a suspension of the normal document destruction procedures, such as a merger or acquisition, or bankruptcy.

A. When does the duty to preserve evidence arise?

The duty to preserve evidence arises as soon as an organization is aware of facts or circumstances that would lead to a conclusion that litigation is imminent or should otherwise be expected. The mere fact that litigation regarding a topic (such as a product or contract) is a general possibility is ordinarily not enough to trigger preservation obligations. What is important to remember is that the duty to preserve can attach well before the organization is served with a complaint or receives formal notice from a plaintiff's attorney.

Example: *Zubulake v. UBS Warburg LLC.*⁴¹ In an employment discrimination case, the duty to preserve evidence attached as soon as plaintiff's supervisors became reasonably aware of the

³⁹ 2000 WL 1694325 (N.D.Ill. Oct. 23, 2000).

⁴⁰ 169 FRD 598 (D.N.J. 1997).

⁴¹ 220 FRD 212 (S.D.N.Y. 2003).

possibility of litigation. In the court's view, that occurred *before* the employee filed a complaint with the EEOC, because there was evidence that "almost everyone associated with [plaintiff] recognized the possibility that she might sue." Although the employer had arguably been merely negligent, the court held that the destruction of emails was willful and gave an adverse instruction to the jury.

Example: *Stevenson v. Union Pac. R.R.*⁴² Where defendant railroad was aware that accidents resulting in death or serious injury were likely to result in a lawsuit and that audio tapes were the sole source of particularly relevant evidence, appellate court affirmed determination that it was bad faith to destroy the tapes after learning of such an accident, even prior to litigation being commenced.

B. Who should impose a litigation hold?

Ideally, a retention policy should identify a point person responsible for implementing and managing a "litigation hold." Communication of the need to suspend normal destruction procedures is critical. A policy should identify:

- (1) the person authorized to impose a legal hold
- (2) the person responsible for communicating the legal hold requirements
- (3) the person responsible for implementation
- (4) the person with authority for determining that the need for a legal hold no longer exists
- (5) how potentially responsive information will be identified
- (6) the person responsible for identifying the information
- (7) where and how information subject to the legal hold will be stored
- (8) what metadata must be preserved
- (9) whether legacy or backup media need to be preserved

C. Tailoring the litigation hold to the circumstances.

A legal hold should be limited in scope to only that information and records that may be relevant to the litigation. Even when a litigation hold is required, an organization is not obligated to immediately "freeze" all electronic information.⁴³

⁴² 354 F.3d 739 (8th Cir. 2004).

⁴³ *See, e.g., Wiginton v. Ellis.* ("A party does not have to go to 'extraordinary measures' to preserve all potential evidence. . . . It does not have to preserve every single scrap of paper in its business.")

An organization generally must use “reasonable efforts” to preserve relevant information. This may require a modification of the organization’s automatic deletion programs or backup procedures for business continuation or disaster recovery. While backup tapes are generally considered “inaccessible” under the new federal rules, an organization still may have an obligation to preserve them, especially if there is no other media containing information from the relevant timeframe. In general, the steps that an organization takes in implementing a litigation hold will be relevant when a court must determine whether routine deletion occurred in “good faith” such that the “safe harbor” from sanctions is available.

D. How to communicate a litigation hold.

- (1) Make sure notice comes from senior management. Courts want to see that an organization has taken a litigation hold seriously and that upper management are actively involved.
- (2) Make sure the notice is sufficiently specific. The notice does not have to be overly detailed, but sufficient to place employees on notice regarding the type of information that must be retained.⁴⁴
- (3) Make sure the notice reaches the key people. The notice does not need to be sent to every single employee. However, it needs to reach the necessary people.⁴⁵
- (4) Make sure the notice is sent to relevant third parties. Sometimes third parties have relevant documents that are effectively under the “possession and control” of the organization. A example of such a third party is an outside auditor or financial consultant.
- (5) Make sure the notice is resent periodically. Employees need to be reminded. Courts have specifically recommended that employers repeat notices of litigation holds.⁴⁶
- (6) Make sure the litigation hold directives are documented. To ensure that an organization will be able to take advantage of the “safe harbor” protections of the new federal rules, they must be able to show a court that they have taken “good faith” steps to adhere to a document retention policy.

⁴⁴ *Id.* (initial notice sent to employees to preserve documents that pertained to only one named plaintiff in class action was insufficient because it did not reflect appropriate scope of preservation obligation).

⁴⁵ *See In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 FRD 598 (D.N.J. 1997) (criticizing email notice to employees that did not contain bolded phrases like “DO NOT DESTROY DOCUMENTS,” mention the specific pending litigation or possibility that failure to comply could result in sanctions, and where not all employees had access to email).

⁴⁶ *See, e.g., Zubulake v. UBS Warburg LLC*, 2004 WL 1620866 (S.D.N.Y. July 20, 2004).

3. Hallmarks of Effective Electronic Discovery Plan

An effective electronic discovery plan will include:

- (a) A current inventory of all sources, collections, and locations of electronic data and all individuals who have access to the data.
- (b) An understanding of the electronic storage, backup, and purging processes and how they can be temporarily suspended.
- (c) An identified group of individuals who will serve as the electronic discovery response team. The team should include, at a minimum and to the extent they exist, a member of senior management, a representative from the IT department, a representative from the legal department, and outside counsel.
- (d) A means of quickly identifying, preserving, and collecting all potentially discoverable data.
- (e) A means of quickly and effectively communicating the preservation and collection obligations to all responsible employees.
- (f) A method for ensuring compliance with the preservation and collection obligations.
- (g) A method for maintaining and monitoring compliance with these obligations through litigation.
- (h) A method for thoroughly documenting and recording the process of identifying, preserving, collecting, and producing the electronic discovery. Tracking chain of custody is particularly important.
- (i) Identification of the person who can serve as the deposition witness on electronic data storage issues.

C. THIRD-PARTY VENDORS

Although an organization may be capable of identifying and taking necessary steps to preserve electronic data, it may not recognize the most efficient means of accomplishing the tasks. Third-party vendors that specialize in electronic discovery and litigation support may be able to provide technical assistance, storage, expert witness, and search capabilities that far exceed anything the organization can do on its own, and at a fraction of the cost.