WHITE PAPER: BEST PRACTICES FOR LEGAL HOLDS

symantec™

Confidence in a connected world.

Best Practices for Enforcing Legal Holds on E-Mail and Electronic Data through Proactive Archiving

Sponsored by Symantec

Jennifer Kehoe Esq.

Best Practices for Enforcing Legal Holds on E-mail and Electronic Data through Proactive Archiving

Sponsored by Symantec

Contents

Abstract

Recent court decisions and new laws have imposed greater obligations on organizations and their legal counsel to preserve many types of electronically stored information (ESI). The rapid growth of technology has only added to the problem. Moreover, failure to preserve e-mail and other electronically stored information has led to severe sanctions against several organizations. The courts have held that failure to preserve ESI can amount to the "spoliation" (or spoiling) of evidence, effectively destroying another party's ability to have their day in court.

However, proper ESI management can both preserve the necessary documents and mitigate any sanctions by showing "good faith" in anticipation of calls for discovery. This paper discusses the situations which might cause an organization to reasonably expect litigation as well as the legal hold policies it should have in place. These should cover all ESI and its location—whether, for example, the information is in a central storage server or scattered in desktops, laptops, removal storage, etc. The paper then reviews the impact of recent guidelines from the Advisory Committee on the Federal Rules of Civil Procedure. In particular, it covers the role of individuals within an organization and the organization's IT and legal counsel—both in terms of preserving documents and in providing testimony.

Finally, the paper concludes by discussing the monumental difficulties of preserving e-mail and outlines the advantages of an archival strategy such as the one provided by Symantec Enterprise Vault™ with Symantec™ Discovery Accelerator. Together, they help ensure that all relevant e-mails, files, and SharePoint and instant messaging data are captured, preserved, and stored in an easily accessible and searchable archive. As a result, the combination can serve as a key component of an organization's overall legal hold policy.

Best Practices for Enforcing Legal Holds on E-Mail and Electronic Data through Proactive Archiving

The world of discovery in litigation is quite different from how it was just a few years ago. Corporate counsel, outside counsel, and corporate executives are all facing significantly larger and stricter duties than in years past, due both to the ever-increasing use of technology, and to changes in the law. The opinions issued in the case of *Zubulake v. UBS Warburg LLC* are well known to anyone who deals with discovery, particularly discovery of electronically stored information (ESI). *Zubulake* and its progeny (including the 2006 amendments to the Federal Rules of Civil Procedure) all impact an organization's obligation to preserve data related to actual or reasonably anticipated litigation. In light of the many and varied difficulties and costs that may be related to preserving all relevant data, organizations are evaluating their own processes for implementing legal holds. If they are not doing so, they should be.

The problems arising with ESI preservation and storage invite technological solutions, including e-mail archiving, that can relieve many of the costs, burdens, and risks associated with identifying, collecting, and preserving ESI in the context of litigation or investigation. As discussed below, many of the costs and risks associated with data preservation and electronic discovery may be lessened by implementing management solutions.

I. Legal background: How did we get here?

One of the principal drivers of the new federal e-discovery rules, discussed below, has been the increase in frequency and severity of e-discovery sanctions. That is, parties have increasingly been sanctioned, or punished, for failure to preserve electronic documents that are relevant to pending or reasonably foreseeable litigation. This duty to preserve information, including electronic information, that is relevant to pending or reasonably foreseeable litigation is the cornerstone of all our discovery rules. In the law, a party that violates this obligation is guilty of what the law calls "spoliation" of evidence. Very simply, this means that one party has spoiled the other's ability to have their day in court by destroying important potential evidence. Where this happens, courts have held that they have a responsibility to act, in order to level the playing field.

Sanctions for spoliation of electronic records have been on the rise. This has been due in large part to the changing responsibilities of organizations and counsel and to the decreasing willingness of courts to give a pass to parties that do not have control of their own information. The leading cases in electronic discovery sanctions, together with the 2006 Federal Rules amendments, give guidance to parties on what courts expect and how parties can meet those expectations.

A. The cases: *Zubulake* and *Coleman*

Zubulake, an otherwise ordinary employment case that became a landmark, gained national notoriety because of one party's inability to produce relevant ESI during discovery. That party's failure to preserve e-mail and other relevant ESI resulted in a $29 million verdict against it. Zubulake underscored, in a series of decisions, the need for changes to the federal rules regarding electronic discovery and foreshadowed some of the implications of those changes.

In one of the opinions, known as *Zubulake V*[1], the court discussed the following steps that corporations and their lawyers should take at the outset of litigation to meet their duty to preserve electronic documents:

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

Second, counsel should communicate directly with the "key players" in the litigation—*i.e.*, the people identified in a party's initial disclosure and any subsequent supplementation thereto. Because these "key players" are the "employees likely to have relevant information," it is particularly important that the preservation duty be communicated clearly to them. As with the litigation hold, the key players should be periodically reminded that the preservation duty is still in place.

Finally, counsel should instruct all employees to produce electronic copies of their relevant active files. Counsel must also make sure that all backup media which the party is required to retain is identified and stored in a safe place.[2]

All of these specific obligations fall under a more general rule that counsel must be familiar with the client's document management system and document retention policies, and with the people who use it.

[1] 229 F.R.D. 422 (S.D.N.Y. 2004).
[2] Id. at 433-34 (internal citations omitted).

Zubulake is probably the single most influential opinion or series of opinions affecting e-discovery, and Judge Scheindlin's guidelines on the roles of both counsel and organizations have been cited and followed by numerous jurisdictions.

Another significant case is *Coleman v. Morgan Stanley*[3], which involved a separate issue of ESI discovery: that of ESI that could not be located, rather than ESI that had been destroyed. During the course of discovery, the court found that Morgan Stanley, after repeated orders from the court, did not locate or search all of its backup tapes for relevant e-mail. Morgan Stanley initially said it had no backup tapes containing e-mail from the requested time period. When this was proven to be untrue after repeated hearings on the matter, the court sanctioned Morgan Stanley via a partial default judgment and by a partial reversal of the burden of proof at trial for the most significant claims. At its most basic, this harsh sanction meant that instead of the usual case where the plaintiff needed to prove that Morgan Stanley had committed fraud, it became Morgan Stanley's burden to prove that it had not committed fraud. The jury awarded the plaintiff $604 million in compensatory damages and $850 million in punitive damages. After adjustment by the court, the final award was $1 billion, 758 million—an award that was later overturned on appeal.

As these cases illustrate, courts believe that litigants—especially corporate litigants—are "fully on notice" of their common law obligations to preserve ESI that is relevant to pending or reasonably foreseeable litigation, and of the fact that the failure to do so is punishable by very severe sanctions indeed. This means that it is imperative, very early on, to issue and enforce a viable legal hold that prevents of loss of relevant ESI. Where large volumes of unstructured ESI such as e-mail and Microsoft® Office files are concerned, vaulting technologies should be seriously considered as being reasonably necessary to help solve what is essentially a problem created by technology itself.

B. The 2006 amendments to the Federal Rules

Before the *Zubulake* case was even filed, the Advisory Committee on the Federal Rules of Civil Procedure began investigating possible amendments to the Rules that directly impact electronic discovery in 1999. These proposed Rules were not published by the Advisory Committee, however, until August 2004. As such, the proposed Rules relating to electronic discovery in many ways reflected familiarity with and adoption of certain holdings in the *Zubulake* case. After extended revisions and multiple public hearings, the amended Rules became effective on December 1, 2006.

[3]2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005), further opinion 2005 WL 674885 (Fla. Cir. Ct. Mar. 23, 2005).

The amended Rules affect numerous electronic discovery issues and will have a significant impact on litigation in federal courts. Organizations need to fully understand their systems, and must be able to communicate that information to their counsel. Counsel, in turn, must be able to process that information and communicate it to opposing counsel and to the court. Counsel need to understand their obligations to provide accurate information about information storage and retrieval systems at the outset of litigation. IT professionals and records management specialists will be called upon to help manage and coordinate these issues. Courts will need to exercise greater oversight at the outset of litigation to ensure that electronic discovery disputes do not overshadow the underlying substantive legal disputes.

With respect to preservation of data and the issuing of a legal hold, although it has long been recognized that when faced with reasonably anticipated litigation or investigation, a company has an obligation to preserve potentially relevant evidence in its possession, custody, or control, including e-mail,[4] one of the notable areas of change in the amended Rules is that, for the first time in the history of the Civil Rules, the word "preservation" appears.

The Advisory Committee notes recognize, however, that preservation of electronically stored information presents significant challenges: "The volume and dynamic nature of electronically stored information may complicate preservation obligations. The ordinary operation of computers involves both the automatic creation and the automatic deletion or overwriting of certain information. Failure to address preservation issues early in the litigation increases uncertainty and raises a risk of disputes."

C. The impact of the amended Rules

What do the amended Rules mean for organizations and their counsel? First, it means that organizations should act now to create or revise a reliable inventory of their electronic information systems and architecture. Understanding where the organization's ESI resides is critical to identifying and preserving relevant information. To achieve this step, organizations should consider identifying these five things:

1. The types of technology the organization uses (*e.g.*, e-mail, databases, voicemail) and the purposes and internal use of each;
2. The systems and software used by the organization in the regular course of business, and any additional formats in which information may be retrieved or produced;

[4] A company's obligation to preserve electronic evidence is not dependent on a preservation order of the court, preservation demand from the opposing party, 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).

3. Backup or archiving systems: what means the organization uses to store older information, how long that information is kept, and how accessible that information is;
4. Recent or planned system changes or upgrades; and
5. The identification of computers and related equipment used by employees, including desktop and laptop computers, PDAs, removable hard drives, etc. that may be used for or contain relevant material

Second, it means that organizations must have a legal hold process in place before litigation starts. The legal hold process must cover the elements of notifying affected employees, as well as using processes and tools to capture and preserve electronically stored information.

Third, it means that organizations must be prepared to describe their electronic information systems as well as their preservation steps at the early conferences. This may include identifying (a) whether the organization's information management and retention program includes automatic destruction components; (b) whether the organization has taken measures to preserve potentially relevant voicemail, e-mail or other ESI, what those measures were, and what date those measures began; and (c) whether specific individuals are responsible for implementing and overseeing a litigation hold, and whether those individuals or others are monitoring compliance with the litigation hold. This will, as a general matter, require a greater awareness of such systems by in-house and outside counsel.

Fourth, as noted by the Advisory Committee, the new rule may mean in appropriate cases that the "identification of, and early discovery from, individuals with special knowledge of a party's computer systems may be helpful." Organizations, therefore, should take steps to identify who in the organization may be the Rule 30(b)(6) witness on the topic if required.

Fifth, the organization must be prepared to explain why onerous or broad preservation demands are unduly burdensome and unnecessary. Indeed, the Advisory Committee anticipates that the preservation discussion will address the preservation steps in the context of each particular case, as they noted that "The parties' discussion should pay particular attention to the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities." The Advisory Committee added that "The parties should take account of these considerations in their discussions with the goal of agreeing on reasonable preservation steps."

> Prior to litigation, a business should (a) develop a document and information management policy that involves key executives and information technology

> staff; (b) ensure that its document and information management policy addresses electronic information; (c) incorporate litigation hold (preservation) procedures in its policy; and (d) develop a litigation hold team that includes information technology personnel, records managers, and in-house and outside legal counsel.

Scheindlin & Redgrave, "Discovery of Electronic Information," *2 Business and Commercial Litigation in Federal Courts 2d* § 22.3 (Robert L. Haig ed.) (West Group and ABA 2005)

The fighting issues, even after these new rules, include, among others: (1) what is "reasonably foreseeable" litigation, and when does it "trigger" a duty to preserve electronic records; and (2) what role does "intent" and "bad faith" with respect to the destruction of electronic records play in the imposition or severity of sanctions imposed.

II. Areas of concern regarding legal holds

Because each organization's ESI use and methods are different, there is no "one size fits all" plan for preservation and production under a legal hold. However, several considerations arise for virtually all organizations regarding preparation for and acting under a legal hold.

A. What triggers a legal hold?

Preservation obligations generally begin when legal or regulatory action is "reasonably anticipated." Although there are no clear rules for when such anticipation begins, some examples of triggering events include filing of a complaint, receipt of a discovery request or subpoena, institution of an investigation by a government agency, knowledge of incident resulting in injury, a court order to preserve, or a claim filed with a government agency. An organization may also trigger its own duty to preserve when it begins to consider filing an action against another party.

B. What is the scope of a legal hold?

Again, there is no straightforward answer to this question that can always be applied. The scope of a legal hold will vary widely from case to case, even within the same organization. Instead of a bright-line rule, there is recognition that the law requires good faith and reasonable steps to preserve evidence. Generally, an organization is not required to freeze all ESI, but instead to take steps to retain and locate existing ESI. Three questions the company and its counsel should

consider are: (1) whose ESI must be retained; (2) what ESI must be retained; and (3) where are such documents and data located? Having a plan in place ahead of the time a legal hold begins will help resolve all three of these questions.

C. What must an organization do to demonstrate good faith in implementing a legal hold?

The most important factor in demonstrating good faith, as discussed above, is having and complying with an existing records and information management program before litigation begins. Such a program should include provisions on how to implement a legal hold, and the organization should document any time a legal hold is put into place. If an organization is able to demonstrate that it had and followed procedures, it is much less likely to be sanctioned for discovery misconduct than an organization without such procedures or the ability to demonstrate them.[5]

III. How organizations can put technology to work for them

Just as technology has created a number of the complications that are inherent in e-discovery, technology can also ease some of the burdens of e-discovery. Searchable, user-friendly platforms of various types can streamline large portions of the preservation and production process. However, it is important to remember that these technological tools do not operate in a vacuum, and that they cannot be effective without underlying policies regarding their use and purpose within each organization. Technology is a tool, not a panacea.

A. Inventory your ESI

Organizations need to put plans in place now, rather than at the start of litigation, in order to meet the obligations under the amended Rules 16 and 26 and investigate and identify all sources of potentially relevant information (*i.e.*, data stores), including, but certainly not limited to, legacy data, backup media, portable media, and remote or third-party locations under its custody or control.[6] It is also advisable to identify and understand IT policies and procedures for managing data, some of which may need to be modified or suspended in order to meet preservation obligations if and when they arise.

However, before any organization can put a plan in place, it needs to understand how ESI is used within its organization, what sorts of information is communicated only via ESI, and how

[5] A recent survey of sanctions decisions (by Judge Shira A. Scheindlin of the United States District Court for the Southern District of New York) suggests that two important factors in the severity of sanctions are (1) the relevance of the electronic evidence that is destroyed; and (2) the level of culpability of the party in its destruction.

[6] Organizations need to be aware that "under its custody or control" does not simply refer to physical custody, and information in the possession of a third party may still be considered by a court to be under the control of the organization.

and where users store ESI. An e-mail archiving solution alone is not a complete solution for many organizations. Organizations need to ask several additional questions when considering how e-mail archiving may work for them:

- **What information do we have, and where is it stored?** Sources may include databases, networks, computer systems, including legacy systems (hardware and software), servers, archives, backup or disaster recovery systems, tapes, disk drives, cartridges, laptops, personal computers, Internet data, PDAs, handheld wireless devices, cell phones, pagers, and voicemail.
- **How is information saved, and by whom?** Organizations may archive everything, or may use backup tapes only for disaster recovery. Individual users may have sole responsibility for preserving all of their own information.
- **Where and how are various types of information stored?** If certain types of data are stored exclusively in one format or location (or, conversely, in all manner of forms and places), it is essential that the organization be aware of it. Legal holds will generally relate to specific dates and topics, and a well-prepared organization will know the first places to search for such information.[7]

B. Understand the role of users

Organizations generally require some individual user assistance in order to comply with legal hold requirements. Most records and information management programs require users to exert some control over records within their custody. Reliance on users for all retention requirements, however, carries risks, particularly if users are the sole custodians of some information. The most obvious risk is that of noncompliance, either intentional or negligent. Users may not understand the legal hold process or may not fully understand their particular obligations. There is no guarantee of consistency when preservation depends on individual users.

[7] As always, this does not free the organization from searching other reasonable locations, but it gives an organization both a good starting point and evidence of good compliance.

Some individual user assistance is necessary, especially in organizations that do not restrict use of personal data stores, such as home computers, PDAs, cell phones, or removable hard drives. In such situations, individual users may be the only sources for searching and preserving some information. Further, the legal hold process should always include notices to all individuals who could potentially have relevant or responsive information. However, individual users should not be the main source for collection.

C. Address e-mail and archiving

Many organizations are looking for ways to deal with e-mail, as it is used in the vast majority of companies, and is often the primary form of communication among employees. One common e-discovery issue arises where e-mail is not centrally stored and managed on the firm's network server (*i.e.*, the only copies of responsive e-mails are located on the individual hard drives of multiple employees' personal computers or laptops). Complying with one's preservation and disclosure obligations can get especially complicated for an organization when the individual employees' computers use a variety of different e-mail programs or when individuals have archived e-mails in .PST or .NSF files or on removable media.

One proposed solution for reducing an organization's burdens with respect to e-mail preservation is the implementation of an enterprise-wide e-mail archiving system. That system may also be associated with an electronic discovery tool that enhances an organization's ability to locate potentially relevant data as well as to effectively and reliably implement a legal hold that affects electronic data. Archiving is a storage strategy that automatically offloads certain data (e-mail, instant messaging files, e-mail attachments, and other electronic documents) to a storage server. This allows an organization to remove the ESI from its main or message servers while still storing relevant material at a lower cost. The extent to which data is saved in the archive, how often, and for how long can all be tailored to an organization's individual needs and the variety of technological solutions offered by archiving vendors.

One important characteristic of an effective e-mail archiving system is its ability to retrieve records based on user-defined searches. The ideal archive will allow for easy, accurate, and fast full text searching. Ideally, the system will also employ intelligent search capabilities that will allow users to perform context searches in their quest to get to the heart of a matter.

A solution such as Symantec Enterprise Vault™ and the accompanying Symantec™ Discovery Accelerator work together to help ensure that all relevant e-mails are captured, routed, and stored on easily accessible and searchable media such as WORM disks, optical devices, and tapes. Implementing a technological solution such as Symantec Enterprise Vault and Symantec Discovery Accelerator can control the costs of responding to discovery requests and can reduce counsel's anxiety over preservation obligations. Some of the benefits of an archiving system include:

- **Centralized retention of messages**—Automated or scheduled archiving promotes ongoing collection in a centralized location. This creates a single, centralized repository that helps to ensure that no data is lost, including legacy PST files and backups, without having access to disaster recovery sources.
- **Searching and sorting capacities**—The ability to automatically search and sort the content of e-mail messages and files eases production obligations during legal holds and collections, from the initial review on. In addition, classification tagging provides continuity between matters.
- **Automation of certain legal hold steps**—In addition to centralizing information for each matter, multiple legal holds (both closed and ongoing) can be tracked in one place. Later holds can build on prior holds, all of which are retained in the system.
- **Tailoring of legal hold processes**—Conversely, an application such as Symantec Discovery Accelerator can be used to preserve specific information for particular legal hold needs in a granular manner, depending on the circumstances.
- **Documented process**—Use of archiving (as with other retention and management systems) provides a record of the steps taken by an organization to comply with its preservation and hold obligations.

Although an archiving system can bring some of the above benefits, it is neither infallible nor a complete solution to legal hold preservation and retention. Organizations must use these systems in conjunction with an overall legal hold policy, and must use them as appropriate for their particular needs. Archiving is not a substitute for ongoing, tailored, and monitored legal hold programs.

A potential pitfall of an archiving system is the potential to over-retain and to archive everything, which can negate many of the intended benefits. The point of preservation is to retain what is or may be necessary, but not to retain *everything*.

IV. Conclusion

With the proper procedures and technological systems in place, an organization can substantially decrease its litigation-related costs and anxieties. That organization can also rest assured that it is properly positioned to comply with the 2006 amendments to the Federal Rules of Civil Procedure. In addition, organizations will be better equipped to locate and search through potentially relevant data that has been preserved pursuant to the specified qualifications of the legal hold. Organizations and their attorneys then can be freed to focus on the merits of the litigation. Regardless of the tools an organization chooses to preserve and maintain its ESI, all organizations must establish a preservation and production method *before* they think they need one.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec logo, and Enterprise Vault are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries. Other names may be trademarks of their respective owners.
10/07 12999214