

THE FIRST FRONTIER

Your First Obligation - Manage, Identify and Preserve the Electronic Evidence

By Michael Arkfeld

Growing Business and Government Information Risk

Electronic information is both ubiquitous and essential to the operation of businesses and government agencies alike. This universal adoption of technology has so drastically improved collaboration and communication across large organizations that it seems almost unthinkable that business could have been done any other way. However, these efficiencies carry with them byproducts in the way of significant risks and obligations that can threaten the budgets, legal reserves and reputations of organizations if not properly and proactively managed.

Under the common law, all organizations have an obligation to identify and preserve electronic evidence when litigation is “reasonably anticipated”, as well as a duty to prevent its spoliation.

Herein lies the rub: “electronically stored information” (ESI) can be changed, overwritten, or obliterated by nor-

Couple this with the increased volume of data, disorganized record retention schemes, widely dispersed locations of ESI and automatic purging systems for electronic data and it can easily lead to a corporation unwittingly contributing to the body of caselaw on this subject with its very own published spoliation opinion, complete with sanctions and adverse inference jury instructions for its trouble.

This is unlike the preservation of information in paper-based discovery, where the information is physically stable. Due to the ease in which electronic information can be destroyed, special attention must be paid to the management and preservation of an organization’s potentially relevant ESI that may have to be produced one day.

If the producing party delays or improperly implements the preservation process and data is destroyed, they will have to contend with an angry requesting party that has many court decisions imposing sanctions and outright default judgment for failing to preserve ESI in its corner.

The courts are not reluctant to impose sanctions for failing to identify and preserve data. *In re Prudential Ins. Co. of Am. Sales Practices Lit.*, 169 F.R.D.

ESI is dynamic and can be changed, created and deleted without the user’s knowledge

mal everyday use. The routine acts of recycling backup tapes, booting up a computer, opening a file, adding new data onto a hard disk, or running a routine maintenance program on a network can permanently alter or destroy existing data without the user’s knowledge. Ken Withers, *Computer Based Discovery in Civil Litigation*, 2000 Fed. Cts. L. Rev. 2 (2000); *In re Tyco Sec. Litig.*, No. 00-MD-1335, 2000 U.S. Dist. LEXIS 11659, at *9-10 (D.N.H. Jul. 27, 2000) (“[plaintiff] has produced evidence that large corporations typically overwrite and thereby destroy electronic data in the course of performing routine backup procedures”).

598, 615 (D.N.J. 1997) (*Prudential* fined \$1 million for its “haphazard and uncoordinated approach to document retention” and not acting quickly to prevent the destruction of electronic data). Courts will examine very closely any destruction of records, after a duty to preserve has been established. Sanctions range in severity from monetary fines, dismissal, default judgment, adverse inference jury instructions, rebuttable presumption jury instructions, preclusion of evidence, preclusion of experts and/or lay witnesses and other sanctions which are only limited by the court’s imagination. One all-too-common “sanction” a party in this situation may find themselves enduring

ing is entering into an unfavorable settlement based on discomfort resulting from this subject, or the costs associated with the actual e-discovery process.

In two landmark decisions, the Courts in *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, 2005 WL 67071 (Fla. Cir. Ct. Mar. 1, 2005), *rev'd on other grounds*, 955 So.2d 1124 (Fla. 4th CA 2007) and

These organizations must have procedures and policies in place to issue “litigation holds” for regulatory investigations or legal discovery requests. Businesses and agencies need to proactively retain live data (e.g., e-mails and IM), as well as legacy data (e.g., tape backups and paper), when litigation is “reasonably anticipated” and the ESI is responsive to the case.

ESI can be changed, overwritten, or obliterated by normal everyday use.

Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (D.N.Y. 2004) issued adverse inference jury instructions as a result of spoliation. As a result, the jury in the *Morgan Stanley* case levied 1.4 billion dollars in compensatory and punitive damages and in *Zubulake* the jury issued 29 million dollars in damages. Both cases involved a failure to properly implement a “litigation hold” and failure to produce relevant evidence from *backup tapes*.

The New Rules

On December 1st, 2006, changes relating to “electronically stored information” (ESI) in the Federal Rules of Civil Procedure took affect. The changes to Rules 16, 26, 33, 34, 37, 45 and Form 35 provide strong language regarding the preservation, production, accessibility, and costs associated with retrieving ESI. These changes will impact virtually every case in federal court.

The primary driving forces behind the implementation of the new rules were:

- The volume of ESI is significantly greater than paper;
- ESI is dynamic and can be changed, created and deleted without the user’s knowledge;
- Systems that create, store and transmit ESI are often complex; and
- ESI may need to be preserved, restored, or processed before it can be reviewed for privilege, trade secrets or responsiveness.

Information Risk

During discovery, an attorney may find out that their client organization has failed to properly implement a “litigation hold” and has error-prone systems and procedures in place for ESI retention and management. This situation can lead to the undesirable outcomes discussed above.

However, many of these organizations are unaware of their information risks and their preservation obligations. A survey conduct-

ed by the American Bar Association’s Litigation Section revealed that:

- Eighty-three percent said that their clients had no established protocol for responding to discovery requests, and only 5.8 percent said that protocols were being developed;
- Sixty-eight percent said that their clients rarely, if ever, took steps to prevent automatic overwriting processes for relevant electronic data; and
- Seventy-six percent said that 30 percent or more of their clients were unaware that electronic information could later become evidence.

PricewaterhouseCoopers/Section of Litigation of the American Bar Association, *Pulse Survey, Digital Discovery and its Importance on the Practice of Litigation* (May 15, 2000).

With escalating pressure being placed on businesses and government agencies by the courts and lawyers today, information retention and electronic discovery management must become a key concern to department heads, IT managers and middle management.

The primary driver of electronic record management is risk mitigation. Unstructured and unmanaged ESI presents a real threat to businesses and government agencies, and this risk is growing every day as e-mail and other types of electronic data continue to gain momentum as business tools. A secondary driver calling for effective record management: the fact that I.T. must cope with unchecked data growth often without commensurate growth in the I.T. budget. These two drivers combined make proper and proactive record management a virtual necessity for large and medium size enterprises.

Document Retention Policy

For a variety of reasons, organizations create and store electronic records. Primarily, it enables an organization to retrieve information that is supportive of the goals and mission of the entity. In addition, organizations will maintain records to comply with existing regulatory and other legal mandates. As a result, most companies have informal and formal document retention systems to ensure that records are available for the organization's purposes and to comply with legal obligations.

The United States Supreme Court has recently reaffirmed the fact that document retention policies are legal. "Document retention policies,' which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business." *Arthur Andersen, LLP v. United States*, 125 S. Ct. 2129, 2135 (2005). The court noted that, "[i]t is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances." *Id.* at 2135.

However, in a commercial litigation case, the defendant failed to preserve e-mail and a spoliation inference would be given to jury and the court was quick to point out that record retention (and thus record destruction) policies must be suspended when the duty to preserve arises. The Court noted that, "The duty to preserve potentially relevant evidence is an affirmative obligation that a party may not shirk. When the duty to preserve is triggered, it cannot be a defense to a spoliation claim that the party inadvertently failed to place a 'litigation hold' or 'off switch' on its document retention policy to stop the destruction of that evidence." *MOSAID Techs. Inc. v. Samsung Elecs. Co.*, 348 F. Supp. 2d 332, 339 (D.N.J. 2004).

A typical document retention program involves the systematic review, classification, retention and, ultimately, the destruction of electronic and paper records. To manage data effectively, a company needs a reasonable document retention policy. An ill-conceived and unreasonable document retention program will subject a company to severe legal exposure, if responsive data to anticipated litigation is destroyed or if needed for compliance mandates.

The primary problem with document retention systems is that ESI is often stored in a disorganized manner, difficult to classify or retrieve and rarely deleted. Users treat inexpensive hard drives and other storage media as bottomless receptacles into which data is saved and rarely purged. This can get expensive when lawyers have to sort through this data for litigation or compliance purposes, much of which may be irrelevant to the dispute. The true cost of processing and filtering electronic information is not the technology involved, but the costs of having attorneys review the information for privilege, responsiveness, etc. The human costs associated with electronic discovery can be substantial, the presence of which can defeat the purposes of a fair, just and speedy resolution of the dispute. For this reason, if the company manages its ESI in an effective way, it will substantially reduce future litigation costs.

Litigation Readiness

e-discovery focuses on identifying, preserving, collecting, processing and reviewing electronic data for disclosure. This involves more than gathering relevant ESI, it includes working with your client in advance of litigation

Seventy-six percent said that 30 percent or more of their clients were unaware that electronic information could later become evidence.

to determine what ESI is being created and what is retained. Then, if litigation occurs the organization will be prepared to issue the necessary litigation hold to preserve relevant ESI.

Make sure your litigation hold procedures include rules for all relevant ESI, such as e-mail, electronic documents, scanned documents, and backup tapes. To aid in turnaround time for the discovery process and reduce the overall expense of the process, document management technology should be employed in the enterprise. This can include email archiving software, document management software, or a combination of both. These tools can apply retention rules as well as create a central searchable repository for locating ESI that may be subject to a litigation hold. This data can then easily be quarantined by moving it to a secure litigation repository. In addition, select a vendor ahead of time to handle data restoration from tapes and for other e-discovery processing functions.

Organizations should have a complete IT map of potentially relevant data that can be provided to outside counsel if litigation is anticipated. This should include not only e-mail servers and backup tapes, but any ESI source including data on systems no longer in use, ESI in remote or third-party locations, other lawsuit data, etc. This blueprint of available ESI will prove invaluable for your attorney's 26(f) "meet and confer" session.

Producing ESI involves many of the same legal principles and strategies that are employed in requesting ESI. It will require you to

understand how computers work as well as how information technologies are used in your client's personal or business life. During this process you need to provide proactive advice to your client as to the preservation, cost and scope of production, as well as current document retention policies. Assembling a cross functional task force (Legal, I.T., HR, RM, etc.), and employing trained consultants to educate and prepare this team is an excellent way to get started.

Summary

Let's face it; it is extremely difficult to properly place a litigation hold on potentially responsive ESI, once litigation is "reasonably anticipated." How can an organization, in a timely and comprehensive manner, contact all custodians, determine the scope of ESI that may be

relevant to a cause of action, preserve the data and then properly collect and produce it? To complicate things further, pulling off this magic act must also be done in an environment where the slightest misstep might lead to inadvertent deletion or spoliation of data on one hand – and inadvertent production of privileged data to an adverse party on the other.

However, there is hope. The solution lies in technology,

ESI may need to be preserved, restored, or processed before it can be reviewed for privilege, trade secrets or responsiveness.

especially since it is technology that caused this problem in the first place. Today, we have the capability to instantly search gigabytes of information in seconds, as long as it is in an organized and protected format. Organizations across the country have to accept the demise of backup tapes and other media that is "not reasonably accessible" and have responsive ESI available for immediate searching and preservation to fulfill their preservation obligations. This, coupled with properly written and applied document retention policies, will result in lower risk, and ultimately, time and cost savings. The I.T. cost savings via more efficient and reduced storage should help executives in the enterprise endorse this strategy. The failure to implement a proper document retention program and allow for immediate access and preservation of ESI has, and will continue, to lead to severe court sanctions.

EMC²
where information lives®

EMC², EMC, and where information lives are registered trademarks of EMC Corporation.

All other trademarks used herein are the property of their respective owners.

© Copyright 2007 EMC Corporation. All rights reserved. Published in the USA. 11/07