



James P. Harris
Direct dial: 603.627.8152
Fax: 603.641.8731
jharris@sheehan.com

Good Company

The Brave New World of Document Retention and Destruction

Friday, January 26, 2007

In the post-Enron world, corporate executives frequently employ euphemisms such as “document retention policies.” In truth, these policies address both the retention and destruction of company documents. The term “document destruction” conjures negative images of employees huddled over shredding machines under the cover of darkness. In 2005, however, the Supreme Court of the United States reversed a criminal conviction against Arthur Andersen, Enron’s accountant, based upon Andersen’s decision to order its employees to destroy Enron documents after Enron’s financial problems became public. The Court spared Arthur Andersen because it acted pursuant to a valid, written document retention policy. [1]

Most companies have document retention/destruction policies, but surprisingly few companies have policies that deal explicitly with electronically stored information (“ESI”). Failing to implement policies governing the destruction, deletion and overwriting of ESI carries serious consequences in today’s legal environment.

Recent changes to the Federal Rules of Civil Procedure, rules that govern litigation in federal courts, heighten the need for companies to be proactive and formulate ESI retention/destruction policies. The amended rules, which went into effect on Dec. 1, 2006, expressly recognize ESI as a form of discoverable information in litigation and require litigants to discuss the preservation and production of ESI at the outset of each case. To effectively meet these requirements, litigants must have full command of the content, location and format of their ESI, as well as the ability to quickly assess whether any ESI is confidential or privileged. Fundamentally, a company’s lawyer must be able to communicate effectively and knowledgably with the client’s information technology managers.

The amended rules also permit parties to request that ESI be produced to opponents in a particular format. A litigant might not be able to simply print spreadsheets and produce them in hardcopy (which eliminates the risk of revealing confidential and potentially damaging meta-data); [2] litigants might be forced to carefully preserve the spreadsheets in their original format and produce them electronically along with its hidden data. Failing to preserve ESI can result in severe sanctions, including the dismissal of a party’s claims.

Apart from these consequences, a defensible document retention/destruction policy makes good economic sense. The sheer volume of ESI that most companies generate exponentially increases the

legal costs incurred to review documents before production in litigation. Document retention/destruction policies that limit the volume of available ESI may save tens of thousands of dollars in litigation costs down the road.

In short, companies must have both document retention and destruction policies, and policies that directly address ESI, in order to meet the needs of business in the ordinary sense and the new demands of litigation. These policies must be understood by managers throughout an organization.

WHAT ARE THE NECESSARY COMPONENTS OF AN ESI RETENTION/DESTRUCTION POLICY?

- First, the policy must address the motivations of those who will be asked to implement it on a daily basis. Human nature is to keep, rather than destroy, all business documents and communications. This motivation is exacerbated by the seemingly low costs to store ESI. High-level corporate executives must galvanize the process from drafting through implementation to ensure all employees buy into the program.
- Drafters of ESI policies must collaborate with IT professionals. A company cannot draft an effective ESI policy without understanding the types of data created by its employees and where such data is stored. Companies must create a list of all sources of ESI (including home computers and external media used by employees) and all forms of ESI (such as e-mail communications, word-processing documents, spreadsheets, databases, and CAD designs). The list must identify past, current, and predicted future technologies, and must be amended each time new technology is added. The policy must cover the lifespan of ESI from its creation through its storage to its destruction. The policy must also consider the retention of old or outdated technology required to access data solely through peripherals that will be obsolete in the near future.
- The policy must include explicit destruction schedules for each form of ESI. A policy might call, for example, for all non-essential email communications to be purged after 60 days. It is helpful to create a quick reference guide along with the detailed ESI policy so employees can refer to the guide for most business records.
- The policy must address the destruction of the underlying electronically stored information and all archived copies. An email deleted from a user's computer remains a record of the company if a version of the record remains saved on a back-up tape or in an archive format.
- The ESI policy must dovetail with the non-ESI portion of the company's document retention/destruction policy. For example, routine destruction schedules must account for the fact that email communications addressing personnel matters are likely considered part of the subject employee's personnel file and therefore must be retained for specified periods of time under federal and state employment laws. Similarly, employers in regulated industries who have obligations to report to government agencies must craft their ESI policies to satisfy any applicable laws.
- Importantly, the policy must address the special concerns that ESI raises for the effective implementation of a so-called "litigation hold." When a company has actual knowledge that it is to be made a party to a lawsuit or reasonably anticipates that a dispute may result in a lawsuit, all destruction of documents that are potentially relevant to that suit must cease. The ESI policy must include mechanisms for communicating suspension of ordinary, scheduled destruction and the steps to preserve ESI until the claim or dispute is resolved. Once a litigation hold is in place, the company must catalog the steps it has taken to ensure compliance, must periodically audit and monitor its employees to ensure diligent implementation, and should require employees to certify periodically that they are implementing the hold. Employers must train their employees in advance to execute a litigation hold, and this includes training to ensure proper maintenance of ESI.

Document retention/destruction policies addressing ESI are not a luxury; these policies are now necessary for nearly every business. The risks for not having a detailed policy are great. Although there are several common ingredients to all ESI policies, they should be drafted with care and must be tailored to the specific business and technologies employed.

This article is intended to serve as a summary of the issues outlined herein. While it may include some general guidance, it is not intended as, nor is it a substitute for, legal advice. Your receipt of Good Company or any of its individual articles does not create an attorney-client relationship between you and Sheehan Phinney Bass + Green or the Sheehan Phinney Capitol Group. The opinions expressed in Good Company are those of the authors of the specific articles.

[1] In the *Arthur Andersen* case, the Supreme Court endorsed destroying documents pursuant to a valid document destruction policy “absent extraordinary circumstances.” The phrase “absent extraordinary circumstances” tracks the inherent tension between legitimately destroying stale business records and sanctionable spoliation, or destroying evidence when one knows, or should know, of potential litigation. In short, one cannot destroy documents when a dispute is on the horizon, when those documents bear in any material fashion on the dispute.

[2] “Meta-data” is hidden information in an electronic document that identifies the computer or computers on which the document was created or revised and the dates and times of creation/revision. In some document-types it can also reveal prior iterations of the document (such as where a “redlining” tool was used as part of the document’s creation) or embedded comments that were removed from the document’s final form.