

WHY YOUR COMPANY NEEDS A DOCUMENT RETENTION POLICY

By Andrew R. Schulman, Esq.

June 8, 2005

A few years ago I represented a small company with just two employees and two computers. Because it did most of its business over the internet, the company sent and received innumerable emails. When it was sued, the company was asked to produce all emails that related to the plaintiff's transactions. Although there were only five transactions, it was extremely burdensome to locate all of the relevant electronic documents. Indeed, some of the most important documents had been deleted long before the lawsuit was filed or contemplated. The company did not have a document retention policy, or even a set of standardized practices. Emails and other documents were simply deleted the way a homeowner might discard old cable bills and junk mail.

At the end of the day, the company had to relinquish its hard drives and pay tens of thousands of dollars to a forensic computer specialist to retrieve "deleted" documents. Worse, the plaintiff was ultimately allowed access to *gigabytes* of information which only became discoverable as a result of the inquiry into the company's record keeping practices.

My client got off easy. In 2003, a federal court in New York ordered an investment bank to pay approximately \$250,000 to search its computer back-up tapes for emails relating to a former employee in a gender discrimination case. The original emails had been deleted even though the lawsuit was foreseeable.

In many cases, courts have allowed juries to take adverse factual inferences against a company that deleted or destroyed documents when litigation was reasonably foreseeable. Depending on the case, such adverse inferences can effectively amount to a directed verdict. In the widely publicized Arthur Andersen case, one of the largest accounting firms in the world was criminally prosecuted for, among other things, failing to retain documents that might have

become relevant in an expanding SEC investigation.

As all of these examples illustrate, in today's world a company that takes a casual or *ad hoc* approach to document storage and retention is putting itself at risk. The time to develop a document retention strategy is now. It will be too late to do so after your company has been sued or become the focus of a government investigation.

The First Rule

The first rule in document retention is to safeguard any document that may be relevant to pending or anticipated litigation or government investigation. Even small companies need to have procedures in place to stop the routine destruction of relevant documents once the company is placed on notice of potential litigation or investigation. Word needs to travel to all affected employees and it needs to travel quickly. In an employment discrimination case, emails on numerous employees' desktops may be relevant. In a software development dispute, the most important documents may prove to be internal company emails and electronic drafts of documents. Even a routine collection case may turn on a series of emails.

Because it is often difficult to know in advance what types of documents will become relevant in subsequent litigation or investigation, you should proceed cautiously in destroying any documents. This means, among other things, consulting in-house and outside counsel at the earliest possible dates. Then, act quickly to advise all relevant employees of the existence and scope of the litigation hold.

Other Rules

Documents that are not subject to a litigation hold should be retained and later discarded pursuant to a well thought out policy. In many industries federal and state law impose strict record keeping and retention practices.

There may also be record keeping requirements imposed by industry-wide accreditation standards or even by clients or customers. You are probably already familiar with the laws and standards that affect your particular business. Nonetheless, you should take a fresh look at all government imposed record keeping requirements to make sure that your company's policy is in compliance. You should then sit down and consider how long you need to keep various types of records for your own business purposes.

Next you need to decide what to do about the ephemera of day to day office life—emails, rough drafts, handwritten notes, etc. Factors to consider in determining whether to destroy these documents may include: (a) industry specific record keeping requirements; (b) foreseeable litigation or investigation; and (c) the intent in destroying the documents. If you determine that the documents should be destroyed, the best way to do this is to slate these documents for destruction after a set period of time unless there is a particular business reason to retain a specific document. The specific time table will, of course, vary depending on the nature of your business and its industry.

The same is true with respect to your computer's daily or weekly back-up media. Back-ups are necessary in the ordinary course of business. However, you certainly don't want to keep a precise copy of how your computer hard drives looked on each day of your company's business life for the past ten years. If you did, then you might conceivably find yourself searching through this morass in the event of unanticipated litigation.

Finally, you need to decide how to store your documents. In the old days, you simply placed your paper documents in numbered banker's boxes and sent them to a warehouse. Today things are more complicated. You will need to develop an electronic filing system for easy access and indexing of all types of electronic documents. This means, among other things, that documents that were once stored on

many desktops and in various offices will have to be kept in a single centralized location.

In the event of litigation, you will likely be required to absorb the entire cost of locating and producing electronic documents that are saved anywhere on your company's hard drives or back-up media. If you have several offices, hundreds of computers and a file cabinet full of back up tapes, this could be a very considerable burden. Thus the surest way to minimize the cost of document production is to store your electronic documents in a manner that facilitates searching and retrieval.

The good news is that if electronic documents have been deleted in good faith and in the ordinary course of business pursuant to a comprehensive document retention policy, courts are unlikely to require extraordinary efforts at document retrieval. Because deleted documents may still exist on your hard drives, a forensic computer specialist might be able to "undelete" them. However, this is an extremely expensive and intrusive process. Therefore, if a company has put an intelligent document retention policy in place, and acted quickly upon notice of litigation or investigation, the courts are reluctant to order a search for deleted materials. Further, in the unlikely event that such a search is ordered, courts are far more likely to shift the cost of this forensic examination onto the opposing party.

A Word About Email

This is an article about document retention, not document creation. Nonetheless, you should caution your employees that anything they write in an email (either within the company or to outsiders) may one day be discoverable in litigation. The same is true with respect to instant messages, although these are often not recorded. Therefore, your employees should be required to use the same degree of professionalism in their electronic communications as in their business letters. While you can't delete embarrassing or unprofessional emails after notice of a lawsuit, you can certainly instruct your team not to write such materials in the first place.

It is also a good idea to share your document retention policy with all employees. They should know that an email they send today will be kept in a readily accessible location for several months (or years) and made available if litigation ensues. They should know that the company keeps back up copies of their emails and that these too will be retained and made available in the event of litigation or investigation. That knowledge should serve to make your employees think twice before drafting and sending inappropriate messages.

Conclusion

While devising and implementing a sound documentation policy may take a little effort, failing to do so may prove to be costly and burdensome. Now is the time to act. It will be too little and too late if you start planning after litigation or investigation becomes foreseeable.

For additional information on drafting document retention policies and related issues contact **Andy Schulman** at (603) 634-4300 or aschulman@gstss.com.