Designing a Compliant Record Retention Policy for Your Business

This article first appeared in the International Technology Law Association's eBulletin, Volume 2, Issue 3, summer 2008.

by Jenna Leavitt

Jenna Leavitt
Senior Associate
IP & Technology Litigation
213.488.7459
jenna.leavitt@pillsburylaw.com

Ms. Leavitt focuses her practice on intellectual property litigation and transactional work, technology and Internet-related matters. She has advised clients on the maintenance, enforcement and defense of intellectual property, technology and entertainment-related rights and in the identification, selection, clearing, registration, protection and licensing of intellectual property, technology and entertainment-related rights.

With the increased reliance on computers, electronic information has become extremely important in litigation. This article deals solely with the policies implemented prior to litigation, not after, such as litigation holds or issues regarding electronic discovery ("e-Discovery"). Electronic mail (email) messages, instant messaging, blogs, chat room transcripts, databases, word processing documents, spreadsheets, deleted documents, web browser favorites, and cache are just some of the electronic information that can be maintained by a business. In fact, recent surveys show that more than 90% of all documents produced since 1999 are in electronic format.

Electronic documents are easier and cheaper to copy, distribute and store than paper documents. For example, exact duplicates of electronic documents can be created at the touch of a button, without regard to the length of the document or the cost of creating the printed copy. In fact, there is general agreement today that the volume of electronic information greatly exceeds the volume of information kept in paper format.

So, how do you maintain this information, especially if you will need to produce it in response to an audit or litigation in the future, or if you simply need it later to help defend prior decisions or actions of your business? Alternatively, retaining all of your business' records indefinitely is not only burdensome and expensive, but can create a hotbed of liability risks.

"Records management, or RM, is the practice of identifying, classifying, archiving, preserving, and destroying records."[1] [1] With the passage of the Federal Sarbanes-Oxley Act (including criminal penalties) in the summer of 2002 and the amendment of the Federal Rules of Civil Procedure in December 2006, businesses have been paying increased attention to the storage and retrieval of electronic records. Retention policies have become a hot topic. Until these new rules and amendments, record retention policies had mostly been ignored. Not only do Sarbanes-Oxley and the Federal Rules require knowledge of the storage and retrievability of electronic records, many other Federal and local statutes do as well. Thus, not having a record retention policy can lead to disastrous results. Further, having a written retention policy allows for the freeing up of valuable storage space, as records are routinely deleted pursuant to the policy (and applicable law).

So, how does your business go about creating a retention policy?

Often, the first step is to meet with the information technology department to learn where and how electronic information is created, stored, archived and destroyed. In addition, the business' organizational structure should be taken into account when reviewing the information, as different departments may be subject to regulations. Once the information and types are located, a policy can be drafted that will directly address the information that is being created. Next, review with the legal department or outside counsel what information should be maintained and for how long, and what information can be destroyed.

Just because there are new rules regarding electronic information doesn't mean that you have to save it all. The rules don't actually prohibit the implementation of a record retention policy, which includes destruction of information after a set period of time. However, be careful, as the new rules do require that such a policy be suspended once there has been a notification of litigation, or litigation is reasonably anticipated.

A retention policy usually contains certain provisions, such as: a statement as to the purpose of the policy, whether the policy will be for the entire organization or a certain department, an exclusion from the policy for litigation or audit purposes, the name of the employee(s) or department(s) responsible for overseeing the policy; the name of the employee(s) or department(s) responsible for destruction pursuant to the policy, and a description of the types of records along with the retention schedule. Additional considerations can include specific instructions for how the records will be maintained (e.g., boxes labeled for off-site storage to be picked up every Friday; backup tapes to be stored in fire proof box and locked in fire proof safe nightly) and how they will be destroyed (e.g., hard drives sent for shredding after written approval received from legal; paper documents approved for shredding and disposed of by a third-party shredding company).

Retention Issues

What documents need to be maintained and for how long?

As many businesses are subject to many regulations, it is important to review what regulations affect your specific business. Never use a generic retention policy, as it may not meet your needs. For example, most generic retention policies call for the destruction of emails after 90 days. However, certain regulations require you to maintain emails for periods of several years. In addition, since the statute of limitations on certain actions can exceed five years, documents which might be relevant to a particular action – such as terminated employees – should be kept for a minimum of five years, regardless of a shorter legally-mandated retention period. Thus, you should develop a retention policy that not only addresses the applicable legal rules and regulations, but also meets your specific organizational and industry needs.

To be effective at retention, you must know where your records are stored. Not knowing can prove to be especially dangerous, as most large dollar sanctions have involved the sudden appearance of documents not known to exist earlier in the litigation. By creating the "map" of information, you can effectively delineate retention management to the correct people. Then, if a document request is served, you know which people have what information without having to search the entire business for it. For example, IT personnel can handle email retention, while HR would maintain employment records.

Another hot area for litigation is compliance with your record retention policy. Just having a policy isn't good enough. You must actively audit to ensure that the policy is being followed. For example, employees may delete their emails once a week even if business policy states that emails should remain on the inbox on the network server for a period of 90 days. By not enforcing the business' policy, you have now let potentially relevant emails be destroyed and could be sanctioned by a court for such non-compliance, even though a litigation hold had not yet occurred.

Destruction Issues

Records retention policies are not just about retention. An effective retention policy allows for the routine destruction of certain records after a set period of time. The policy should set forth the retention time period as well as how the record will be destroyed once the time period has expired.

So, how do you "destroy" your records once your policy's retention time period has expired?

Most businesses will simply delete the information from the hard drive and consider it "destroyed." However, for the most part a deleted file is not, in fact, "destroyed." As most computer-savvy people know, it is virtually impossible to completely destroy an electronic document. The most common reason for this is the method in which computer operating systems delete files. Generally, an operating system renames the file and removes it from the computer's "directory." Then, it designates the physical space on the hard drive to be overwritten by new information. The problem is that most of the time, the physical space is not actually overwritten, thus the deleted file can be recovered. If it appears that electronic information may have been deleted, and it may be responsive to a document request or relevant in litigation, it is important to quickly bring in a qualified computer forensic specialist to retrieve the information to prevent any further destruction by overwriting with new information.

A recent study of used hard drives being sold on the Internet found that 80% of the drives still had recoverable information. So, if you are going to dispose of a hard drive, you need to make sure that it's done correctly. Taking a hammer to the drive, or drilling a hole (or multiple holes) in it, is not likely enough to make the data unrecoverable. While it may make the hard drive inoperable, it rarely makes the data stored on the drive unrecoverable. Companies are now offering hard-drive shredding, which completely destroys the data on a hard drive; the end process involves completely melting all the particles within the drive. While inexpensive, the shredding is only an option if you can afford to constantly purchase new hard drives. Otherwise, you must find a way to delete the data, but allow for reuse of the drive.

Another option for destruction of media such as hard drives or backup tapes is "degaussing." Degaussing equipment is often used by the government to destroy its records. Data is stored in magnetic media, such as hard drives, tapes and diskettes (floppy disks), by making very small areas change their magnetic alignment to go in a certain direction. Degaussing equipment applies a strong magnetic field to the media, effectively destroying it because it removes the magnetic alignment. Again, this process is only useful if you can afford to continually purchase new storage media. Further, there is no way to be sure that the degaussing was successful. There is no log file created, so you cannot use this process if you must be compliant with certain federal regulations, such as the Health Insurance Portability and Accountability Act ("HIPAA") (related to personal medical information) or the Gramm-Leach-Bliley Act (relating to personal financial information), which specify how data destruction must occur and be tracked.

There are several commercial products for sale that will "delete" information stored on a hard drive so that it is not likely to be recoverable. These programs, often called "scrubbers," work by using a technique which deletes the data and then overwrites it with random data several times. The Defense Department recommends that the data be overwritten at least seven times before a drive is discarded. However, the use of scrubbing software can be detected, so be sure there is no litigation hold in place and your retention policy allows for the destruction before commencing.

Destruction may also be a problem when it involves corrupted media. For example, corrupt hard drives and backup tapes cannot be erased. Thus, shredding or degaussing are the only options for completely removing the information. When moving forward with information or media destruction, be sure to check as to whether the media can be truly erased, or whether it needs to be destroyed.

Once you have a policy in place that allows for the destruction of information, you need to be careful as to who does the actual destruction. Delegating the destruction of records may be a difficult task, as it can sometimes be a simple task that management may feel too qualified to perform (e.g., the shredding of documents). However, because most of the records contain sensitive information, or information that would be of value to competitors, having upper management or a specialized outside company perform the destruction is generally recommended. Non-management employees often have an economic incentive to maintain the information, rather than destroy it, as is evident by the numerous lawsuits involving theft of trade secrets by companies against former employees.

Systems

Once you have a record retention policy in place, the next step is to make sure that it is properly implemented. There are now several commercial systems that can help you do so. These systems not only assist in the maintenance, storage and destruction of paper records, but also use technology to capture, store, archive, and sometimes destroy your electronic information. A simple Google search for "record retention systems" or "document retention systems" will yield numerous vendors. Further, many of your current backup systems already contain programs that allow for the retention of electronic information (in addition to the programs to implement tape backups).

Data Structures and Organizations

The portability of digital documents has dramatically increased the number of locations where electronic information may be found. Typical information is stored in places such as desktop computers, laptops, network servers, personal digital assistants ("PDA"), and, possibly, home computers. A computer may have several versions or copies of the same document on its hard drive, while other versions or copies may be located on a network server. Still other versions or copies may be downloaded on other desktop hard drives other than the desktop of the file creator. The document also may have been copied onto diskettes, CD-ROMs, USB flash drives, or other digital media, and there may be copies on a laptop or PDA.

In addition, there may be copies or versions on an employee's home computer(s), either transferred via the Internet or by traditional portable media.

Further, most businesses protect their electronic information by duplicating it onto digital storage media (backup media) on a regular schedule for disaster recovery purposes. This creates yet another set of copies of the document. By business policy, the backup media generally should be retained for only a few days or months, and then it should be destroyed or recycled and reused in the course of subsequent backups. However, in practice, even if there is a destruction or reuse policy, the electronic information often remains on the backup media for much longer than the prescribed policy period, so audits must be done to ensure compliance.

As stated above, understanding the basic flow of information throughout your systems allows for more accurate retention and destruction of information. There are numerous sources which can contain electronic information. For example:

- Emails
- Internet browser information (cached files, cookies, download records)
- Word processing documents, spreadsheets, presentations
- Instant messaging/chat records
- Efaxes
- Electronic calendars
- Voicemail
- Text messages
- Blogs
- Chat room/bulletin board postings

Emails

For example, many businesses rely on email as their primary form of communication. The current volume of email communications is astonishing. For example, a business of ten employees who receive 10-15 emails a day would generate approximately 36,000-54,000 email messages a year. And, unlike telephone conferences and face-to-face meetings, the entire nature of the email communication is preserved in a written record that can be retained. Generally, email is considered the most damaging of the electronic documents, as it tends to encompass more "smoking gun"-type information and communications. This is partially because employees don't seem to understand that business email is not necessarily as private as they think, but rather it is a permanent and discoverable business record.

Internet Browser Information

Another often forgotten area of electronic information is Internet information. For example, Internet bookmarks or favorites files provide a listing of the user's favorite web sites, cached files record the Internet address of web pages visited, cookies contain information about the user to a particular web site that are used for quick recall when the user revisits the web page (including web beacons or web bugs which are usually transparent images that monitor the behavior of the web site user), and information regarding files downloaded. Such files can serve as substantive evidence of wrongdoing (such as copyright infringement) and present circumstantial evidence of wrongdoing (such as pornography).

Chat Rooms

Chat rooms and bulletin boards are places where users can go to communicate with each other. Businesses can host such chat rooms internally, for employee use, or externally, for membership and/or public use. They usually contain central areas for each topic of discussion and organize posts (messages sent to the room) in a threaded matter usually by date, subject matter, or author. Although chat rooms and bulletin boards can hold information that is crucial to a case, such as defamatory postings, they present logistical problems for retention. Complete transcripts of conversations or postings are seldom kept for more than a few days, so as to clear the disk space for new conversations or postings, as most web site space is limited (much more so than internal business storage). Be sure to include such information in your record retention policy so that there are no misconceptions as to how long the information will be maintained. After deletion, records may be limited to a user's participation in a conversation or posting, based on the user's log-in records, which are usually stored longer than the actual text of the conversation.

Blogs

One of the newest forms of electronic communication is what is commonly known as a blog—which is short for the term "web log." A blog typically serves as a publicly accessible personal journal for an individual or company. Blogs are generally updated daily, as the success of a blog is largely determined by the availability of up-to-date, current information. Blogs are usually like chat rooms or bulletin boards in that they maintain information for short periods of time to free up space for new information. Again, be sure to include a blog in your record retention policy, as blogs have become a hot topic in the litigation arena.

Other Communications

Other forms of electronic communication include instant messaging, text messaging, voicemail, and electronic collaboration. Instant messaging is a type of communication that creates a virtual private chat room that allows two or more people to communicate with each other real time over the Internet. It is largely a text-based communication that creates a written record. Text messaging typically uses cellular telephones or PDAs to send text-based messages from one party to another. Text messaging communications are generally limited to a few hundred words due to the memory and size limitations of the receiving devices. Text messages can often be sent from web sites, leaving a trail of information. Voicemail is an often overlooked electronic communication. Voicemail systems are now generally computer-based systems which maintain electronic information regarding voicemail messages in computer files. Thus, voicemails should be stored in a manner similar to emails. Electronic collaboration includes such things as virtual post-it notes, virtual white boards, and web casts, which all create some sort of discoverable written record, and thus should be covered in a retention policy.

Conclusion

The creation and implementation of a policy to retain records, including electronic information, can be daunting, but it is an extremely useful tool in managing your business' information. By understanding how and where information is stored, you can easily obtain relevant information, should the need ever arise. At the same time, an appropriately conceived and carried out retention policy permits your business to conserve resources by freeing up valuable storage space, and to avoid preserving an endlessly large pool of "discoverable" information, while still fulfilling its legal obligations.

[1][1] Wikipedia, http.//en.wikipedia.org/wiki/Records_Management.

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | 1.877.323.4171