



July 2007



Kenneth Sperl
Of Counsel
(614) 360-2023
www.tsibouris.com
ken.sperl@tsibouris.com

ELECTRONIC RECORDS RETENTION

THE NEW RULES

In December of 2006, the Federal Rules of Civil Procedure were modified to address electronically stored information. A business has a duty to preserve potentially relevant information regarding a matter that may be litigated. The business that is the subject of a discovery request in litigation is responsible for the production of electronically stored data, including e-mails, voice mails, instant messages and documents requested by the other party to the litigation that have been preserved in electronic databases. Sanctions and fines can be imposed by the court if the business fails to disclose all relevant data.

The revised rules contain a safe harbor provision that provides protections for a failure to provide data. If the request for information is too burdensome, relief can be requested. If the data being sought has been deleted as part of the normal process employed by the business to destroy data, there can also be relief from sanctions. To benefit from the safe harbor provision of the revised Rules of Civil Procedure, a business

must adopt an electronic records retention policy that is well-conceived, applied consistently and in good faith.

DEVELOPMENT OF AN ELECTRONIC RECORDS RETENTION POLICY

The first step in the development of a records retention policy is to get the wholehearted support of senior management of the business. Without the support of management, the officers and employees of the business may not be enthusiastic participants.

As you begin to develop the policy, you must determine what data to preserve. Not all information should be preserved. Data that should be preserved by a business is called a "record." A record is defined generally as data that is relevant to the activities of the business. For example, an email describing the parameters of a project being conducted by the business should be considered to be a record, while an email among employees to set up lunch is not.

To develop an effective electronic records retention policy, you must involve someone who knows the information technology systems of the business. Developing a comprehensive record retention policy that

requires reworking of the software systems utilized by the business will not be well received by management and may waste valuable resources.

It is also important to involve someone from each business unit of the company, including the human resources department, where there are several very specific document retention requirements. The representatives do not need to be involved in the actual development of the policy, but should advise what records to preserve and how long to preserve them. This helps ensure that it will be utilized once in place.

A business may be tempted to use its backup system as the database to preserve records. This is not a good idea. A backup system calls for a periodic "dump" of all data then on the electronic system of the business without sorting the data. Being able to retrieve the data as efficiently as possible should be one of the primary goals of a record retention policy. Backup systems are not designed to allow easy access in a search for a particular piece of information. They are designed to take a "picture" of the data in the system at one particular point in time. Trying to find an email regarding a particular topic, especially

if the date of the email is not known, might require a review of several backup tapes. The process becomes very time consuming and expensive.

As indicated above, an acceptable record retention policy must be well-conceived and consistently applied. If, for example, one division of the business declares that all emails, regardless of the topic, are to be destroyed after 30 days and another division requires that email be preserved for time periods adjusted by the topic of the email, there is not a consistent application of a retention policy.

Another potential issue regarding the preservation of records occurs when officers or employees retain a record on a desktop computer, on a laptop, on a handheld device, or even in a personal computer at home. If the policy does not prohibit these types of alternative storage for records, the devices might end up being the subject of a discovery request. Often, businesses have policies separate from record retention policies that warn employees that they should have no expectation of privacy in the use of computer equipment supplied by the company. Including directives in the record retention policy that are synchronized with the policies regarding a lack of an expectation of privacy should be helpful in limiting the scope of a search in response to a discovery request.

Deleting records can create liability, but preserving records longer than is necessary can do so as well. A schedule for destruction of records that calls for records to be preserved for only as long as a relevant statute requires, or if there is no relevant statute, for as long as there is a legitimate business need for the record, should suffice.

When a record is able to be purged from the system, privacy and

nondisclosure requirements applicable to the record being destroyed must be followed to prevent a breach of either of those obligations. In situations where a third party is used to store or destroy records, the contract with the vendor should address the requirements that must be employed not only in storing records, but also in destroying them.

LITIGATION HOLD

One of the primary purposes of a record retention policy is to enable the retrieval of electronically stored information without great expense in the event a business is the subject of a discovery order in litigation.

When a business becomes aware that an action is filed or even imminent, records potentially relevant to the matter must not be destroyed. Having a record retention policy in place is a valuable tool to avoid having to freeze the entire information technology system of the business in place at the time the business becomes aware that it has been, or soon will be, sued.

Not only must the record keeper of the business preserve the relevant information, notice must be provided to all officers and employees, directing them to preserve all relevant records. The attorney that will be handling the litigation must collect the records that are related to the matter and review them to determine whether or not they are relevant.

All the records are considered to be privileged information until the attorney completes the review and determines what records are responsive to the discovery request and not subject to privilege. As part of this process

the attorney should order the collection of the back up tapes for the relevant time period. The back up tapes most likely will not become evidence, nor will they be turned over to the opposition, in part because they will contain a significant amount of information that is not relevant to the litigation.

At the conclusion of the litigation, the information in the litigation hold file may be preserved indefinitely, or returned to the normal destruction cycle.

++++
Mr. Sperl has assisted corporate clients with compliance, governance, technology procurement, licensing, and ecommerce.

You may reach him at (614) 360-2023 or ken.sperl@tsibouris.com.

This Privacy and Security Update is intended to provide information about important legal developments, not legal advice. Readers should consult legal counsel for advice about their specific circumstances.