Thomas A. Pendleton

*Thomas A. Pendleton is a partner at the law firm of MacDonald, Illig, Jones & Britton LLP. A graduate in Economics and German from Allegheny College and a graduate of the Vanderbilt University School of Law, he practices in the area of business transactions and related litigation.*

# New E-Discovery Rules Underscore Importance of Record Retention Policies

Federal courts have imposed new requirements for handling electronically stored information (ESI) if a lawsuit is reasonably anticipated or actually filed, and state courts will likely apply similar requirements. This article briefly explains the new requirements and why each business needs to prepare and implement a written policy for properly handling ESI.

Electronically stored information exists in many forms, such as word processing documents, e-mails, voicemails, text messages, pictures, drawings and spreadsheets. This information might be found on a computer network in the office or factory, home computers, BlackBerrys, cell phones and digital cameras, to name a few places.

If a business learns of an actual or reasonably anticipated lawsuit, the business must preserve documents and other information, whether in printed or electronic form, that may be relevant in the lawsuit. The duty to preserve evidence extends to those employees likely to have relevant information, in other words, the key players in the case. This preservation of evidence is often called a "litigation hold."

The purpose of the litigation hold is to suspend routine document destruction policies. In order to properly implement a litigation hold, a business must consider the following criteria:

1. The business transaction or events on which the lawsuit is based;
2. The subject matter of documents and electronic information to be preserved;
3. The locations where electronic information may exist, including home computers or other devices owned by employees to perform company work;
4. The employees who are likely to be "key players" in the litigation; and
5. The key information technology (IT) staff who should be included in efforts to preserve information.

If a lawsuit is reasonably anticipated or actually filed, it is prudent for the business' IT staff to meet with legal counsel to discuss how best to manage this process. A meeting also gives the lawyer the opportunity to learn about the business' practices with respect to electronic information.

To prepare for this meeting, the business should gather information on how and where it stores electronic data, such as: 1.) the individuals who maintain electronic information; 2.) the types of e-mail and file servers used; 3.) backup policies; and 4.) document retention and deletion schedules.

Courts have established some limitations on the obligations to preserve evidence. Litigation does not require a business to preserve "every shred of paper, e-mail, electronic document or backup tape." The preservation obligation generally does not apply to inaccessible backup tapes that are maintained solely for the purpose of disaster recovery.

On the other hand, if backup tapes are actively used for information retrieval, then those backup tapes are subject to the litigation hold. Furthermore, if a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of the "key players" to the litigation should be preserved if the information contained on those tapes is not otherwise available.

The most prudent approach is to err on the side of preserving rather than deleting information. Failing to preserve relevant electronic evidence can have serious consequences if a lawsuit is filed. Courts have entered various sanctions against a litigant for failing to preserve evidence such as: 1.) instructing the jury that the lost evidence would have been unfavorable to the party who lost it; 2.) entering judgment on some or all claims or defenses; and/or 3.) imposing substantial monetary penalties on the parties or lawyers responsible for the loss of evidence.

The new rules mean that every business should have a written policy which describes how electronic information is stored and when it can be destroyed. Employees should be trained in using the new policy, and supervisors should make sure that the policy is being followed. The written policy should require the periodic erasure or destruction of various types of electronically stored information at the end of carefully chosen destruction periods.

*For more information about this issue, contact Thomas Pendleton at MacDonald, Illig, Jones & Britton LLP at 814/870-7756 or tpendleton@mijb.com.*