It's 2007...Do You Know Where Your Data Is?

An Overview of How E-Discovery Rules May Affect Your Business

By Bobby L. Hazelton, Esq.

What should you do with your email and computer systems if you become involved in a lawsuit? How much access will the other side get to your archives of electronic data, recorded voice mails, instant messages, and other computer files? Previously, the answers to these questions were not well defined. Often litigants would face costly court battles before the trial even began to determine each side's obligations for production of electronically stored information. In some cases, litigants were sanctioned with fines and other forfeitures if they did not produce all the relevant electronically stored information.

Now, the rules governing the discovery of electronically stored information, commonly referred to as "electronic discovery" or "e-discovery", are increasingly becoming more formalized. New amendments to the Federal Rules of Civil Procedure governing electronic discovery went into effect on December 1, 2006. The Commonwealth of Massachusetts has published a judicial report advising judges how to interpret the Massachusetts Rules of Civil Procedure for e-discovery.

The initial reaction to the new rules caused a wave of a fear reports by many legal analysts. Many news accounts of the e-discovery rules contained a quote from Alvin F. Lindsey about companies committing "virtual shredding" if they wrote new data over old data on a backup tape. While Mr. Lindsey's assertion may be technically true, the new rules should ease the burden and uncertainty that existed prior to the formalization of electronic discovery procedures. In fact, the new rules provide information on how companies can exempt information that is not reasonably accessible. Nevertheless, the new rules do make clear that companies should have knowledge about where its data is located, and that companies should have a mechanism to place a "litigation hold" on the deletion of data relevant to current and reasonably suspected lawsuits.

The federal e-discovery rules require early disclosure by the parties of the location of relevant electronically stored information. If a company suspects a lawsuit, it should have a mechanism to quickly locate all relevant data, including data that may be stored on phone systems, email systems, data cards, backup tapes, and other information archives. Many software vendors and information technology providers have introduced new tools and services designed to help companies locate and isolate this information. If a company does not have systems and procedures in place to quickly locate data, it should be looking at improving this capability in the near future. Under the new e-discovery guidelines, the ability to craft a legal magic bullet to gloss over a lack of knowledge on the location of data will be greatly diminished. Moreover, locating the data will be the first step necessary to institute a "litigation hold" on the deletion of relevant electronic data.

Companies cannot, and most often should not, delete any relevant data once a lawsuit has been suspected. This does not mean that a company cannot perform routine purges of non-relevant data consistent with an organizational data retention plan. The "virtual shredding" of electronically stored information only becomes an issue once a lawsuit has commenced or is reasonably suspected. Reasonable suspicion would be warranted in any situation where a company has received a formal demand or claim; has knowledge of an accident or an anticipatory breach of contract; has commenced an investigation of some impropriety; or any other action that would normally put the company on notice about a possible dispute between itself and another party.

Disputes are often suspected before the involvement of counsel. A company should have in place its own set of processes and procedures to ensure that relevant data is not deleted. These processes should include both data retention guidelines for Information Technology personnel as well as other key employees that may have data available through offline sources. You do not want an incriminating document to later appear that may have been located on an employee's data card, but not the main computer system.

The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age, published by Pike & Fischer, are rapidly becoming the standards for data retention and deletion. Adopting the Sedona Guidelines helps ensure that relevant information can be isolated and retained immediately after the imposition of a litigation hold. More important, having established a set of prudent best practices can often save costly sanctions or possible forfeiture of a lawsuit. The new e-discovery rules do not require organizations to turn over data that is not "reasonably accessible." Data that has been deleted pursuant to policies and procedures consistent with an emerging industry standard would be less likely to draw sanctions or other adverse actions by the court in the discovery stage of the proceedings.

Once a company has located and preserved the data, it may then work with legal counsel to make determinations on what data must be submitted in the discovery process. Privileges and

other discovery exceptions have not changed as a result of the enactment of the new e-discovery rules. Sorting through the data before final presentation to the adverse party will typically be the last step in the e-discovery process. Although courts often require that the data be presented in its native format, determining what data you have to submit is still paramount. A company should not send an adverse party a full backup of all electronic systems. Full backups may contain valuable trade secrets or other confidential information. In fact, the disclosure of some confidential information could be actionable by other parties. If a company has a legal or contractual duty to keep certain information private, it still must take reasonable steps to prevent an authorized disclosure.

Although you may wish to have an attorney determine what data must be presented, having the data available prior to the involvement of litigation counsel can save a company a great deal of time and money. If you do not know where your data is located, and do not have the ability to preserve relevant information, your case may be lost before an opening argument.

RESPONSIVE SOLUTIONS

Two simple words that explain our commitment to you. Being responsive is a critical element in building a strong attorney-client relationship. Whether you are a new or existing client, we'll be quick to respond to your needs with the knowledge necessary to find solutions to your legal concerns.

www.fletchertilton.com

Bobby L. Hazelton
P: 508.532.8040
F: 508.532.8340
E: bhazelton@fletchertilton.com

Fletcher Tilton PC
Attorneys at law

THE GUARANTY BUILDING
370 Main Street, 12th Floor
Worcester, MA 01608
TEL 508.459.8000 FAX 508.459.8300

THE MEADOWS
161 Worcester Road, Suite 501
Framingham, MA 01701
TEL 508.532.3500 FAX 508.532.3100

CAPE COD
1579 Falmouth Road, Suite 3
Centerville, MA 02632
TEL 508.815.2500 FAX 508.459.8300