E-Column

By Reg P. Wydeven
October 6, 2007

It seems as though anything techno and cool today has the letter “e” in front of it, like e-mail, e-filing, or e-dating. Internet companies even put an “e” in front of their name, such as ebay, eharmony or etoys.

It looks like the legal world has gotten into the e-game as well. The Federal Rules of Civil Procedure, which govern lawsuits filed in federal courts, have recently been amended to introduce new discovery rules for electronically stored data.

Lawsuits can be filed in federal court if the plaintiff is from a different state than the defendant and the amount in controversy is in excess of $75,000.00, or if the lawsuit arises under federal law.

“Discovery” is that part of the litigation process where the parties to the lawsuit obtain information from each other and third parties that will hopefully be helpful in building their case. This information is typically obtained through examinations of witnesses called depositions, written questions called interrogatories, and requests for the production of documents.

The scope of discovery can be very broad. Parties can obtain any information that is relevant to their case or is simply likely to lead to information relevant to their case. Some information is not discoverable, such as information protected by attorney-client privilege.

The revised Federal Rules now address the discovery of “electronically stored information,” or ESI. Coined “e-discovery,” parties can now request that one another produce ESI. ESI includes all current and future types of computer-based information, such as voice mail messages, email messages (including deleted emails), instant message logs, computer documents, temporary files, backup systems and web site logs.

The new rules require parties subject to a lawsuit to provide copies or descriptions of all its ESI. A party requesting ESI may specify the form in which the ESI should be produced.

Parties must now hold a pre-trial conference to discuss and develop a discovery plan. The discovery plan should address the preservation and format of ESI. The plan also identifies ESI that is privileged and not discoverable, and establishes other limitations on discovery. This plan is then confirmed by the judge.

A party does not have to produce ESI if it is not reasonably accessible because of undue burden or cost, such as deleted data. However, this party has the burden of showing the undue burden or cost. A judge can still order the production of the ESI if the requesting party can show just cause, especially if that party is willing to assume any production costs.

Once a lawsuit is filed, companies are required to put a “litigation hold” on all relevant ESI, meaning ordinary destruction measures must be ceased. Companies that destroy ESI can be sanctioned by the court. Sanctions include default judgment, the exclusion of evidence or witnesses, or monetary fines.

A court may not impose sanctions, though, if a company fails to produce ESI because it was lost as a result of routine, good-faith procedures. Accordingly, businesses are strongly encouraged to establish a policy governing the retention and destruction of ESI. For example, if it is a company’s policy to only back up voicemails for one week, the company would not get into trouble if it cannot produce a voicemail message from eight days ago.

Basically, the rules are designed to prevent executives from sprinting to the ‘delete’ button on their servers at the first sign of a lawsuit in a move known as the e-race.