



DESTROYING E-MAIL?

New Federal Rules Apply to Preserving E-Mail, Voice-Mail & Other Electronic Communications

By John W. Traeger

Most business communications occur electronically and are stored in computers, CDs or other electronic devices – unless they are deleted.

But new federal rules effective December 1, 2006, are prompting businesses to seek legal counsel and follow new procedures for preserving virtually all forms of electronic documents, including e-mail and voice mail.

Why? Failure to follow newly amended Federal Rules of Civil Procedure for electronically stored information (ESI) may result in sanctions or stiff penalties for any business facing litigation or pending litigation.

In general, the new rules concern business information generated, stored or transmitted via personal computer, laptop, wired phone system, cellular phone, wireless voice/data devices (such as a Blackberry[®]), and other electronic voice/data communications devices.

As such, the new rules impact word-processed documents (including drafts); e-mail; voice mail; electronic calendar entries; electronic presentations (such as Microsoft PowerPoint[®]); and electronic spreadsheets (such as Microsoft Excel[®]).

Failure to comply may be risky

The U.S. Supreme Court endorsed the new “E-Discovery” rules as amendments to Federal Rules of Civil Procedure in April 2006 and submitted them to Congress, where enactment was approved. In addition to potential sanctions and penalties, risks to firms that do not understand the new E-Discovery rules may include:

- * Disruption of business during a legal discovery process.
- * Damage to a firm’s reputation based on allegations that records were illegally destroyed.
- * Inadvertent disclosure of privileged and confidential information as part of the ESI discovery process.

The result? Many businesses are now implementing ESI management programs to take advantage of the new rules’ “Safe Harbor” provisions. These provisions denote that a party cannot be punished for deleting ESI before the threat of litigation “as a result of the routine, good-faith operation of an electronic information system.” Steps that may help you gain such protection include:

- * Implement new procedures for managing business records, including for retention and destruction of paper and electronic records, which comply with federal and state retention requirements.
- * Consider all business records that may be discoverable in litigation to protect against potential claims and sanctions, including for “spoliation of evidence.”
- * Involve legal counsel and IT specialists to develop new ESI policies and programs.
- * Re-train employees and confirm implementation of new ESI procedures.
- * Monitor federal court decisions interpreting the new rules.

In some ways, the new E-Discovery Rules reflect the Sarbanes-Oxley Act signed into federal law in 2002. Known as SOX, this law introduced regulatory changes into professional accounting practice and corporate governance requirements to help protect corporate investors and shareholders.

Also, the new rules reflect federal regulatory actions taken against U.S. companies for failing to produce electronic data, including e-mail, in the face of investigation or litigation. Such actions resulted in penalties totaling millions of dollars for some companies.

Is this confidential?

Software that archives e-mail, voice mail and other e-communications is available, but simply backing up data is not a solution for compliance with the new rules in the face of potential litigation. Given the huge amount of ESI likely to be transferred during a legal discovery process, it is crucial to have procedures in place to *recover accidentally disclosed privileged information*.

If you are in business, make sure your new ESI records analysis and management plan considers the *full scope* of the new E-Discovery rules. It should contain procedures to place a “litigation hold” on discoverable documents. In addition, it should follow federal and state record retention and destruction periods.

Generally, if a document does not serve a legitimate business purpose and there is no legal requirement to retain it, the document should be destroyed, with the caveat that deleted electronic documents may be recovered by computer forensic experts. An attorney experienced with ESI can provide more information.

It’s true – without electronic communications, business would not function. But the responsibility of analyzing and preserving business communications in today’s world is more important than ever.

*John W. Traeger is a law partner at **Gallop, Johnson & Neuman, L.C.** in St. Louis with extensive experience dealing with federal, state and local regulatory authorities, and with electronically stored records management programs. He can be reached at 314 615 6113 or JWTraeger@gjn.com.*
