The New Federal Rules of Civil Procedure: IT Obligations For Email
(Effective December 1, 2006)

By Roger Matus, Chief Executive, Sean True, Chief Technology Officer, and Chuck Ingold, Principal Research Engineer, InBoxer, Inc.

The U.S. Supreme Court approved on April 12, 2006 what may be the most far-reaching change for the handling of email as evidence in all federal courts. The "Amendments to the Federal Rules of Civil Procedure" (FRCP) have significant impact because, among other things, it defines what is acceptable for discovery and disclosure in legal cases.

Who Does the FRCP Impact?

The FRCP is so important because it effects every business, organization, and person who may ever be involved in a federal court case. Such cases include law suits that cross state lines, actions by the Internal Revenue Service, violations of federal compliance regulations (such as HIPAA and Sarbanes-Oxley), immigration cases, and more.

There are no exceptions for company size or non-profit status. It is difficult to think of a single U.S. entity that could not feel the effects.

How Does the FRCP Impact IT?

The FRCP creates an extremely broad description of what "electronically stored information" must be disclosed, places a time limit for the disclosure, and stipulates a "good-faith" test on retention schedules. The IT department will need to respond more quickly than before to discovery and internal investigation requests. For email, the IT department will need to know the following:

- What email is stored anywhere in the organization.
- How to produce email and how much effort it would take to produce it.
- When and how email may be deleted.

Delays in responding to a request for information can be costly. In one case, the U.S. District Court determined the appropriate fine for a late response to a discovery request was $50,000 per day. While the fine was eventually reduced, it was replaced by severe non-monetary sanctions (Serra Chevrolet v. General Motors).

What Needs to Be Disclosed

The new FRCP requires an exhaustive search for all electronically stored information, including email, that is "in the possession, custody, or control of the party." It must be disclosed "without awaiting a discovery request" (Rule 26(a)(1)). The only exception is for privileged information.

The search must be done at the beginning of a legal case and certainly no later than the first pre-trial discovery-related meeting, which is required to be within 99 days (Rule 16(b)).

As a result of the search, a "copy of, or a description by category and location" of all electronically stored information that "the disclosing party may use to support its claims or defenses" must be presented. In the case of email, this disclosure likely includes every relevant piece of email that may be stored, including back-up tapes employee PCs, or Blackberry devices. (Rule 26(a)(1))

Even if the one party "identifies (information) as not reasonably accessible because of undue burden or cost," its description, category, and location must be disclosed (Rule 26(b)(2)(B)). This means

that the information must be identified, even if it is difficult to retrieve. Nothing can be left out and opposing counsel can challenge.

With a short timetable for the first pre-trial meeting, the urgent demands on IT are significant. For most IT departments that use backups or traditional archiving systems, IT staff may need to be taken off of existing projects with short notice to fulfill the request. Delay is not an option.

It is expected that most emails will need to be produced in their original form, although the companies can discuss the form in which data is to be produced (Rule 26(f)(3)). In a landmark 2004 case, the U.S. District Court ruled that electronic documents must be produced "in native format" and "with their metadata intact." (Williams v. Sprint) Metadata includes message attributes such as file owner, creation date, routing details, the sender, receivers, and subject line.

RECOMMENDATION: Look for a system designed to rapidly retrieve any internal or external email without changing the original message. These systems, like the InBoxer Anti-Risk Appliance, should index every email message, preprocess relevant messages where possible, and provide real-time updates for new relevant mail. It should identify all senders and recipients and it should never change the original message.

Retention Schedules

FRCP Rule 37(f) protects companies from sanctions for deleting email as part of "routine, good-faith operation." This so-called safe harbor provision protects companies that delete email as part of ordinary business activities.

Unfortunately, "routine, good-faith operation" is not defined. The authoritative Advisory Committee on Civil Rules said that an entity would usually be protected if it took "reasonable steps to preserve the information after it knew or should have known the information was discoverable."

An implication of Rule 37(f) is that sanctions may be imposed if email is deleted in bad faith. Certainly, any company with a "delete all email" policy or a 30, 60, or 90 day retention policy for the purpose of destroying "smoking guns" ought to consider whether its policy would stand a court test of "good-faith."

As an extra measure, many companies place a "litigation hold" to prevent the deletion of email from or to employees who may be relevant to a case.

RECOMMENDATION: Review organizational retention policies. Determine whether the policies reflect "good-faith" operations appropriate for the business needs of the organization. Some points to consider in creating a retention schedule appropriate for a business would include relevant compliance regulations, the length of a typical company contract, and the statute-of-limitations for potential federal offenses.

Avoid policies that opposing counsel could claim are solely for the purpose of deleting evidence. Anticipate that short retention schedules may be challenged.

Consider an monitoring and archiving system that can rapidly retrieve and sort email, such as the InBoxer Anti-Risk Appliance. These systems can shorten response time and give a more complete itemization of email messages, which reduces a company's risk under the new FRCP.