



Federal Rules of Civil Procedure: IT Obligations For Email

By Roger Matus, Executive Vice President, Safecore
Sean True, Vice President of Research and Development, Safecore
Chuck Ingold, Principal Research Engineer, Safecore

More than 50 court opinions on electronic discovery have been issued since the Amendments to the Federal Rules of Civil Procedure (FRCP) took effect about a year ago.

These opinions can guide organizations and IT departments about which aspects of the FRCP are really important because the courts often base future decisions on prior opinions. Some of the things IT can learn include the following:

- The courts are no longer tolerant of organizations that have not implemented timely programs to accurately retrieve email.
- Just implementing a policy for retention and litigation hold is not enough. Companies must prove they are enforced at all levels.
- The penalties for failing to meet the FRCP deadlines can be an order of magnitude larger than putting a system in place.
- Limited staff and resources are not excuses for missing deadlines, even for small organizations.

It is difficult to identify a single U.S. entity that could not feel the Federal Rules of Civil Procedure. There are no exceptions for company size, non-profit status, or foreign organizations. The FRCP apply to law suits that cross state lines and many court cases that involve federal regulations, such as workplace safety, immigration, and discrimination. States are also starting to adopt the major provisions of the FRCP for state courts.

CIOs, IT executives, and their representatives can be called to testify under oath about their electronic discovery procedures and the accuracy of the evidence presented. Failure to be accurate can be damaging. In June 2007, a company was sanc-

tioned because their counsel made representations that were based on inaccurate IT information.

This whitepaper will start with a brief examination of five of the more notable opinions related to IT's implementation of the Federal Rules of Civil Procedure. The whitepaper will continue with an overview of the FRCP requirements for IT.

Recent Rulings That Impact IT

Complete Information Expected

During the lengthy anti-trust case between Intel and AMD, Intel said that it set a firm, clear retention policy in place once it learned of AMD's legal intentions. Employees, however, didn't always follow the instructions.

Intel was compelled to search back-up tapes to produce past email messages. Given that Intel has about 100,000 employees who send and receive dozens of messages each day, the total number of messages in a year processed by Intel may exceed 500-million messages per year.

In April 2007, the *Wall Street Journal* reported that Intel "spent \$3.3-million to process computer tapes to help recover missing emails and expects to spend 'many millions of dollars' in the effort."

Deadlines Must Be Met

In *Best Buy v. Developers Diversified Realty*, the defendants argued that the emails and other electronic documents that were demanded by Best Buy were not "reasonably accessible" from Diversified's back-up system. They cited a cost

Safecore's recommendations are all related to products and technologies. Safecore does not give legal advice and disavows any text that the reader might consider to be legal advice.

Please contact competent legal counsel.

of \$125,000 to recover the information, although they did not substantiate the cost.

The judge did not accept the argument and ordered that the information be produced within 28 days, including IT time and legal preparation. According to Law.com, final cost to restore and review the emails and other documents from 345 back-up tapes was an estimated \$500,000, not including attorney fees.

Developers Diversified tried a second time to get an extension, given the size of the effort. But the court upheld the ruling based on the unsubstantiated request and kept the deadlines in force.

This ruling may emphasize the importance of responding to the FRCP's short deadlines and for substantiating claims that the data is not "reasonably accessible."

Lack of Resources

In *Williams v. Taser International*, one of Taser's representations regarded limited resources in a small organization. Taser represented that it made a significant effort to meet court requirements by hiring and training a technology employee specifically to manage the electronic discovery process. As Taser has just 245 employees, according to its web site, hiring a staff member could be seen as significant..

The court, however, did not accept limited resources as an excuse. It stated that it expected the company to make "all reasonable efforts ... including ... retaining additional IT professionals to search electronic databases and adding additional attorneys ..."

This opinion suggests that the courts would not accept a lack of IT resources as a reason for failing to meet the FRCP requirements, even for a small organization.

It is worth noting that this case is a complex wrongful death suit. There were many arguments between the parties over discovery, which complicate the issues and are not covered here.

Preserving Email Evidence

Most organizations know that if it becomes aware of potential litigation, it must preserve possible evidence. This obligation is known as "litigation hold." If an employee deletes a relevant email and there is not a central copy, the company could receive significant sanctions for spoliation.

In *United Medical Supply v. United States*, the government was sanctioned for allowing email to be deleted. There was not a central archive, so the government needed to depend upon employees following policy. A government attorney properly notified those involved to hold email according to the policy.

The problem is that the government did not confirm that all the people involved were actually following the notice. Counsel made representations about what was being preserved based on inaccurate or incomplete IT information. The result was that the court ordered the government to reimburse United Medical Supply for some of their discovery costs and barred them from cross-examining United Medical Supply's expert witness on various aspects at trial.

In *Doe v. Norwalk Community College*, the court specifically cited the defendant's failure to "put a litigation hold in place." The court said that Doe was entitled to an adverse instruction to the jury regarding destroyed evidence. In addition, the court awarded some legal fees and the reimbursement of expert fees. The result probably far outweighed the cost of having a system put in place.

These rulings suggest that creating a policy is not enough. Organizations must confirm that the policies are followed accurately or create a system that insures that evidence will not be lost.

FRCP Requirements for IT

Exhaustive Search

The amended FRCP requires an exhaustive search for all electronically stored information, including email, which is "in the possession, custody, or con-

control of the party.” It must be disclosed “without awaiting a discovery request” (Rule 26(a)(1)). The only exception is for privileged information, such as email between an attorney and client.

The phrase “in the possession, custody, or control of the party” may be the most important phrase in the Rules. “The party” likely includes all employees, executives, directors, Board members, faculty, staff, administrators, and certain contractors. Therefore, if a single “party” has a single copy of an email on his or her laptop computer, even if he or she works hundreds of miles away, that email is under the party’s “possession, custody, or control.”

The Rules do not require organizations to archive electronic information that is not otherwise kept electronically, with the exception of the “litigation hold” provisions discussed later.

Many companies archive email centrally because (1) many employees keep email for long periods of time and (2) it is easier to recover email from one location than from remote laptop computers.

Original Form

It is expected that emails will usually 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.

In general, this means that an organization should be able to deliver electronic copies of the documents, such as email messages. Printed copies and images are not “in native format” and not with “metadata intact.”

When an organization selects between a backup or archiving system, there are three critical items to consider:

- Ensure that you cannot change any of the original messages. For example, if you use an

email client to read an email from a backup, the act of opening the message could change message heading information. This act could spoil an important piece of evidence.

- Ensure that your archiving system does not add information, such as indexing information, to an email. Many archiving systems were designed before the FRCP was amended and may not follow this requirement.
- Ensure that it is easy to export messages and sets of messages in their original format. Some systems make it difficult to export evidence to opposing counsels for use with other systems.

Litigation Hold

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.

However, “good faith operation” also includes the obligation of the party to make sure that employees cannot delete messages once they are put on “litigation hold.”

Specifically, the authoritative Advisory Committee on Civil Rules stated: “Good faith in the routine operation of an information system may involve a party’s intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation”

As mentioned earlier, court opinions show that it is not enough to have a policy in place or to trust employees to keep required information. The courts may require you to prove that the litigation hold was effective, as in *United Medical Supply v. United States*, which was discussed earlier.

A “litigation hold” on should be placed on documents and email when litigation is “reasonably foreseeable.” Some good indicators that a hold is required are as follows:

- A formal complaint, subpoena, or notification of a lawsuit is received.

- Somebody threatens litigation, even verbally by saying, “I am going to sue.”
- A regulatory or governmental body starts an investigation.
- An attorney or third-party investigator requests facts related to an incident or dispute.
- An incident takes place that results in injury.
- An employee makes a formal complaint to management, especially when related to personnel issues.

Deadlines

The exhaustive 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.

The deadline mentioned above is not just for IT. It includes the legal review and preparation of materials for use. Therefore, the actual time available to IT to collect all of the email is much shorter.

With this short timetable, IT departments need to be prepared. 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.

Therefore, archiving systems that take steps to speed up the retrieval process, such as the pre-classification of messages, have significant advantages over those that only index text.

Conclusion

Recent court opinions have emphasized several aspects of the amended Federal Rules of Civil Procedure for IT departments. Perhaps most important is that the courts are no longer tolerant of organizations that have delayed implementation of systems that comply with the FRCP.

Many companies are centralizing the collection of email messages because it is most efficient for meeting deadlines and for complying with Litigation Hold requirements. Email is often archived because individuals keep copies on PC’s in their possession.

Accurate and fast message retrieval is probably the most important consideration for compliance with the Federal Rules of Civil Procedure. As always, consult with your attorney before implementing any program.

For further information, please visit www.inboxer.com, write info@safecore.com, or call 1-781-272-1140 (in the U.K. call 0871-733-6293).

The information contained in this document is for educational purposes only. Safecore does not give legal advice and disavows any text that the reader might consider to be legal advice.

Please contact competent legal counsel.

Copyright 2009 by Safecore, Inc. All Rights Reserved.

Not responsible for errors and all information is subject to change without notice. INBOXER is a registered trademark. Safecore and the InBoxer Glove are a trademarks of Safecore, Inc. All other marks are the property of their respective owners.